FLOSS
MANUALS

Table of Contents

Table of Contents

Table of Contents

Advanced Background

Table of Contents

Table of Contents

Table of Contents

Glossary

Table of Contents

Glossary

Introduction

On 10 December 1948, the adoption by the General Assembly of the Universal Declaration of Human Rights launched a new era. Lebanese scholar Charles Habib Malik described it to the assembled delegates as follows:

> *Every member of the United Nations has solemnly pledged itself to achieve respect for and observance of human rights. But, precisely what these rights are we were never told before, either in the Charter or in any other national instrument. This is the first time the principles of human rights and fundamental freedoms are spelled out authoritatively and in precise detail.* ***I now know what my government pledged itself to promote, achieve, and observe. â ¦ I can agitate against my government, and if she does not fulfill her pledge, I shall have and feel the moral support of the entire world.***

One of the fundamental rights the Universal Declaration described, in Article 19, was the right to freedom of speech:

> *Everyone has the right to freedom of opinion and expression; this right includes freedom to hold opinions without interference and* ***to seek, receive, and impart information and ideas through any media and regardless of frontiers.***

When those words were written sixty years ago, no one imagined how the global phenomenon of the Internet would expand people's ability to "seek, receive and impart information", not only across borders but at amazing speeds and in forms that can be copied, edited, manipulated, recombined and shared with small or large audiences in ways fundamentally different than the communications media available in 1948.

More information in more places than ever imagined

The unbelievable growth in the past several years of what is on the Internet and where it is available has the effect of making an unimaginably vast portion of human knowledge and activity suddenly present in unexpected places: the hospital in a remote mountain village, your 12-year-old's bedroom, the conference room where you are showing your closest colleagues the new product design that will put you ahead of the competition, your grandmother's house.

In all of these places, the possibility of connecting to the world opens up many wonderful opportunities for improving people's lives. When you contract a rare disease on vacation, the remote village hospital may save your life by sending your test results to a medical specialist in the capital, or even another country; your 12-year-old can research her school project or make friends with kids in other countries; you can present your new product design simultaneously to top managers in offices around the world, who can help you improve it; your grandmother can send you her special apple pie recipe by e-mail in time for you to bake it for dessert tonight.

But the Internet does not contain only relevant and helpful educational information, friendship and apple pie. Like the world itself, it is vast, complex and often scary. It is just as available to people who are malicious, greedy, unscrupulous, dishonest or merely rude as it is to you and your 12-year-old child and your grandmother.

Not everyone wants to let the whole world in

With all of the best and worst of human nature reflected on the Internet and certain kinds of deception and harassment made much easier by the technology, it should not surprise anyone that the growth of the Internet has been paralleled by attempts to control how people use it. There are many different motivations for these attempts. The goals include:

- Protecting children from material perceived as inappropriate, or limiting their contact with people who may harm them.
- Reducing the barrage of unwanted commercial offers by e-mail or on the Web.
- Controlling the size of the flow of data any one user is able to access at one time.
- Preventing employees from sharing information that is viewed as the property of their employer, or from using their work time or an employer's technical resources on personal activities.
- Restricting access to materials or online activities that are banned or regulated in a specific jurisdiction, which could be a country or an organization like a school -- explicit sexual or violent materials, drugs or alcohol, gambling and prostitution, and information about religious, political or other groups or ideas that are deemed to be dangerous.

Some of these concerns involve allowing people to control *their own* experience of the Internet (for instance, letting people use spam-filtering tools to prevent spam from being delivered to their own e-mail accounts), but others involve restricting how *other people* can use the Internet and what those *other people* can and can't access. The latter case causes significant conflicts and disagreements when the people whose access is restricted don't agree that the blocking is appropriate or in their interest.

Who is filtering or blocking the Internet?

The kinds of people and institutions who try to restrict the Internet use of specific people are as varied as their goals. They include parents, schools, commercial companies, operators of Internet cafÃ©s or Internet Service Providers, and governments at different levels.

The extreme end of the spectrum of Internet control is when a national government attempts to restrict the ability of its entire population to use the Internet to access whole categories of information or to share information freely with the outside world. Research by the OpenNet Initiative (http://opennet.net/) has documented the many ways that countries filter and block Internet access for their citizens. These include countries with pervasive filtering policies, who have been found to routinely block access to human rights organizations, news, blogs, and Web services that challenge the *status quo* or are deemed threatening or undesirable. Others block access to single categories of Internet content, or intermittently to specific websites or network services to coincide with strategic events, such as elections or public demonstrations. Even countries with generally strong protections for free speech sometimes try to limit or monitor Internet use in connection with suppressing pornography, so-called "hate speech", terrorism and other criminal activities, or the infringement of copyright laws.

Filtering leads to monitoring

Any of these official or private groups may also use various techniques to monitor Internet activity of the people they are concerned about to make sure that their attempts at restriction are working. This ranges from parents looking over their child's shoulder or looking at what sites were visited on the child's computer to companies monitoring employees' e-mail to law enforcement agencies demanding information from Internet Service Providers or even seizing the computer in your home looking for evidence that you have engaged in "undesirable" activities.

When is it censorship?

Depending on who is restricting access to the Internet and/or monitoring its use, and the perspective of the person whose access is being restricted, nearly any of these goals and any of the methods used to achieve them may be seen as legitimate and necessary or as unacceptable censorship and a violation of fundamental human rights. A teenaged boy whose school blocks access to his favorite online games or to social networks like MySpace feels his personal freedom to be abridged just as much as someone whose government prevents him from reading an online newspaper about the political opposition.

Who exactly is blocking my access to the Internet?

Who is able to restrict access to the Internet on any given computer in any given country depends on who has the ability to control specific parts of the technical infrastructure. This control may be based on legally established relationships or requirements or on the ability of governmental or other bodies to pressure those who have legal control over the technical infrastructure to comply with requests to block, filter or collect information. Many parts of the international infrastructure that supports the Internet are under the control of governments or government-controlled agencies, any of which may assert control, in accordance with local law or not.

Filtering or blocking of parts of the Internet may be heavy-handed or very light, clearly defined or nearly invisible. Some countries openly admit to blocking and publish blocking criteria, as well as replacing blocked sites with explanatory messages. Other countries have no clear standards and sometimes rely on informal understandings and uncertainty to pressure ISPs to filter. In some places, filtering comes disguised as technical failures and governments don't openly take responsibility or confirm when blocking is deliberate. Different network operators even in the same country and subject to the same regulations may execute filtering in quite different ways out of caution or technical ignorance.

At all levels of possible filtering, from individual to national, the technical difficulties of blocking precisely what is viewed as undesirable may have unexpected and often ridiculous consequences. "Family-friendly" filters meant to block sexual materials prevent access to useful health information. Attempts to block spam may filter out important business correspondence. Attempts to block access to specific news sites may also cut off valuable educational resources.

What methods exist to bypass filtering?

Just as many individuals, corporations and governments see the Internet as a source of dangerous information that must be controlled, there are many individuals and groups who are working hard to ensure that the Internet, and the information on it, are freely available to everyone who wants it. These people have as many different motivations as those seeking to control the Internet. However, for someone whose Internet access is restricted and who wants to do something about it, it may not matter whether the tools were developed by someone who wanted to chat with a girlfriend, write a political manifesto, or send spam.

There is a vast amount of energy, from commercial, non-profit and volunteer groups, devoted to creating tools and techniques to bypass Internet censorship. Some techniques require no special software, just a knowledge of where to look for the same information. Programmers have developed a variety of more capable tools, which address different types of filtering and blocking. These tools, often called "circumvention tools" help Internet users access information that they might not otherwise be able to see.

What are the risks of using circumvention tools?

Only you, the person who hopes to bypass restrictions on your Internet access, can decide whether there are significant risks involved in accessing the information you want. And only you can decide whether the benefits outweigh the risks. There may be no law specifically banning the information you want or the act of accessing it. On the other hand, the lack of legal sanctions does not mean you are not risking other consequences, such as harassment or losing your job.

About This Manual

This manual 'Bypassing Internet Censorship' provides an introduction to the topic and explains some of the software and methods most often used for circumventing censorship. There is some information on avoiding surveillance and other means of detection while bypassing censorship, however this is a large topic by itself so we have only touched on it where it coincides directly with issues of circumvention.

A full discussion of techniques for maintaining anonymity and preventing detection of content or activities is beyond the scope of this book.

This manual was written in partnership with the **Sesawe** coallition.

What is Sesawe?

Sesawe is an international consortium working to support uncensored access to the Internet. It includes software developers as well as organizations and individuals who share a belief in the need for an open Internet. They include academic research centers, think tanks, nonprofit organizations working on media issues and advocacy groups, as well as dozens of individuals who share these goals. Sesawe is not an organization, it is a gathering place to share information and related resources. Partner organizations are independently managed and financed, and responsible for their own activities.

sesawe
YOUR KEY
TO AN OPEN WEB

Visit the website at https://www.sesawe.net

Authors

This manual has content that was largely written at a Book Sprint. The Book Sprint was held in the beautiful hills of Upper New York State in the US. Eight people worked together over an intensive five-day period to produce the book. It is a living document of course and is available online for free, where you can also edit it and improve it.

In addition to the material written at the Book Sprint, material has been contributed from previous publications. These include contributions from:

- Ronald Deibert
- Ethan Zuckerman
- Nart Villeneuve
- Steven Murdoch
- Ross Anderson
- Freerk Ohling
- Frontline Defenders

These writers kindly agreed to let us use their material within a GPL licensed environment.

This manual has been written within FLOSS Manuals. To improve this manual follow these steps:

1. Register

Register at FLOSS Manuals:
http://en.flossmanuals.net/register

2. Contribute!

Select the manual (http://en.flossmanuals.net/bin/view/CircumventionTools) and a chapter to work on.

If you need to ask us questions about how to contribute then join the chat room listed below and ask us! We look forward to your contribution!

For more information on using FLOSS Manuals you may also wish to read our manual:
http://en.flossmanuals.net/FLOSSManuals

3. Chat

It's a good idea to talk with us so we can help co-ordinate all contributions. We have a chat room for this using Internet Relay Chat (IRC). If you know how to use IRC you can connect to the following:
server: irc.freenode.net
channel: #booksprint

If you do not know how to use IRC then visit the following web based chat software in your browser:
http://irc.flossmanuals.net/

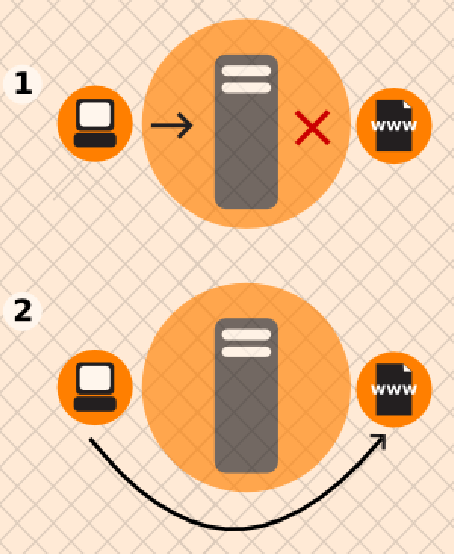
Information on how to use this web based chat software is here:
http://en.flossmanuals.net/FLOSSManuals/IRC

4. Mailing List

For discussing all things about FLOSS Manuals join our mailing list:
http://lists.flossmanuals.net/listinfo.cgi/discuss-flossmanuals.net

Bypassing Internet Filtering

There are a number of methods to bypass Internet filters, including software tools and protected pathways. Collectively, these are called **circumvention** methods and can range from simple work-arounds to complex computer programs. For instance, sometimes it is possible to access a banned Web site just by opening a copy that has been **cached** by a search engine, instead of trying to access it directly.



Circumvention Providers

Circumvention providers are individuals or organizations that provide methods for avoiding filters on the Internet. They can be large commercial organizations that offer circumvention services for a fee or individuals or organizations that provide circumvention services for free. Circumvention providers often install software on a computer in a non-filtered location and then make connections to this computer available to those who access the Internet from a blocked location.

Circumvention Users

Circumvention users are individuals or organizations that bypass Internet filtering using circumvention technologies and usually include people who wish to access or send information from restricted locations. For instance, many Internet users want to protect their identities or activities out of a personal desire for privacy. They may also wish to avoid repercussions from authorities who restrict Internet access -- whether a disapproving parent, an employer, a copyright holder, law enforcement or a government censor.

Am I Being Blocked or Filtered?

In many countries, it is no secret that government censorship of the Internet exists, as documented in the book *Access Denied: The Practice and Policy of Global Internet Filtering*, edited by Ronald Delbert, John Palfrey, Rafal Rohozinski, and Jonathan Zittrain (http://opennet.net/accessdenied). When a popular site is widely blocked, that fact tends to become widely known within the country.

But, in general, determining whether someone is preventing you from accessing a Web site or from sending information to others can be difficult. When you try to access a blocked site, you may see a conventional error message or nothing at all... the behavior may look like the site is inaccessible for technical reasons.

Some organizations, most notably the OpenNet Initiative (http://opennet.net), are using software to test Internet access in various countries and to understand how access may be compromised by different parties. In some cases, this is a difficult or even dangerous task, depending on the authorities concerned.

In some countries, there is no doubt about government blocking of parts of the Internet. In Saudi Arabia, attempting to access pornography results in a message from the government explaining that the site is blocked, and why. In countries that block without notification, one of the commonest signs of censorship is that a large number of sites with related content are inaccessible for long periods of time, except perhaps when they take countermeasures such as moving to a new domain. Another is that search engines return useless results or nothing at all about certain topics. These may be related to pornography, gambling, drugs (including alcohol) or other illegal activities or to political or religious movements deemed dangerous (for example, neo-Nazi sites blocked in Germany).

Filtering or blocking is also done for a variety of reasons that have little to do with politics. Parents may filter the information that reaches their children. Many organizations, from schools to commercial companies to the US military, restrict Internet access in order to prevent users from having unmonitored communications, using company time or hardware for personal reasons, infringing copyrights, or using excessive networking resources.

Detection and Anonymity

The tools to defeat Internet **blocking**, **filtering** and **monitoring** are designed to deal with different obstacles and threats. These tools can improve access to information and people, as well as mitigate risks associated with that access. Different tools may facilitate:

- **Circumventing censorship:** Reading or authoring documents or other kinds of content, sending or receiving information, or communicating with particular people, sites or services while bypassing attempts to prevent you from doing so. For example, reading a page from a Google cache or an RSS aggregator rather than from the original Web site.
- **Preventing eavesdropping:** Keeping communications private, so that nobody can see or hear the content of what you're communicating. (However, they might still be able to see with *whom* you're communicating!) Tools that try to circumvent censorship without also preventing eavesdropping may remain vulnerable to censorship by **keyword filters** that block all communications containing certain prohibited words. For example, various forms of **encryption**, such as **https** or **SSH**, make the information unreadable to anyone other than the sender and receiver.
- **Remaining anonymous:** The ability to communicate so that *no one* can connect you to the information or people you are connecting with â neither the operator of your Internet connection nor the sites or people you're communicating with. For example, anonymous **remailers** and some proxy services, such as **Tor** (when certain anonymity precautions are taken), provide this service.
- **Concealing what you are doing**: Disguising the communications you send so that someone spying on you will not be able to tell that you are trying to circumvent censorship. For example, **steganography**, the hiding of text messages within an ordinary image file, may conceal that you are using a circumvention tool at all.

Some tools protect your communications in only one of these ways. For example, many proxies can circumvent censorship but don't prevent eavesdropping â they let you view a blocked site, but may not prevent someone from monitoring what you are reading. It's important to understand that you may need a combination of tools to achieve your goal.

Each kind of protection is relevant to different people in different situations. When you choose tools that bypass Internet censorship, you should keep in mind what kind of protection you need and whether the particular set of tools you're using can provide that sort of protection. For example, what will happen if someone detects that you are attempting to circumvent a censorship system? Is it important to you to conceal exactly what you're reading and writing about, or do you just want to get access to a particular site or service?

Sometimes, one tool can be used to defeat censorship and protect anonymity, but the steps for each are different. For instance, Tor software is commonly used for both purposes, but Tor users who are most concerned with one or the other will use Tor differently.

An important warning

Most circumvention tools can be detected with sufficient effort by network operators or government agencies, since the traffic they generate may show distinctive patterns. This is certainly true for circumvention methods that don't use encryption, but it can also be true for methods that do use encryption. It's very difficult to keep secret the fact that you're using technology to circumvent filtering, especially if you use a fairly popular technique or continue using the same service or method for a long period of time. Also, there are ways to discover your behavior that do not rely on technology: in-person observation, surveillance, or many other forms of traditional human information-gathering.

FLOSS Manuals cannot provide specific advice on threat analysis or the choice of tools to meet the threats. The risks are different in each situation, and change frequently. You should always expect that those attempting to restrict communications or activities will continue to improve their methods.

If you are doing something that may put you at risk in the location where you are, you should make your own judgments about your security and (if possible) consult experts:

- If you select a method that requires reliance on a stranger, be careful to do what you can to ensure you can trust that person.
- Remember that the promises of anonymity and security made by different systems may not be accurate. Look for independent confirmation.
- Achieving anonymity or security may require you to be disciplined and carefully obey certain security procedures and practices. Ignoring security procedures may dramatically reduce the security protections you receive.
- Be aware that people (or governments) may set up **honeypots --** fake Web sites that pretend to offer secure communication but actually capture the communications from unwitting users.
- Pay attention to non-technical threats. What happens if someone steals your computer or mobile phone or those of your best friend? What if an Internet cafÃ© staff person looks over your shoulder? What happens if someone sits down at a computer in a cafÃ© somewhere where your friend has forgotten to log out and sends you a message pretending to be from her?
- If there are laws or regulations that restrict or prohibit the materials you are accessing or the activities you are undertaking, be aware of the possible consequences.

To learn more about digital security and privacy, read:

http://www.frontlinedefenders.org/manual/en/esecman/intro.html

http://security.ngoinabox.org/html/en/index.html

How the Internet Works

The **Internet** is a decentralized worldwide network of computer networks. Although many people use the terms "the Internet" and "the Web" interchangeably, the Internet is the physical connection of computer networks together with certain methods of communication. The Web is one of many ways of communicating using the Internet. You can also use the Internet for **e-mail**, **file sharing**, **Usenet news**, and **chat**.

Connecting to the Internet

The easiest way to use the Web is often to find a local Internet cafÃ© or telecenter that provides Web access. If you need to set up our own computer with an Internet connection, you would, typically, open an account with an **Internet Service Provider** (ISP). You may need some extra equipment, such as a modem or a **router**, to enable your computer to connect with the ISP.

The ISP in turn may purchase its own Internet access from a national provider (unless it is a branch of a national provider). National providers may similarly receive their connection from one of the multinational companies that maintain and operate the servers and connections that are called the **backbone** of the Internet. The backbone is made up of major server installations at critical points, and global connections between them via fiber optic cables and satellites. These connections enable communications between Internet users in different countries and continents. National and international providers connect to this backbone through special **routers** known as **gateways**, which are connections that allow one network to communicate with another. Gateways, just like other routers, may be a point at which Internet traffic is monitored or controlled.

When you connect to the Internet, your computer is normally assigned a numeric **IP address**, which can be written as four numbers in the range 0-255, separated by dots. Like a postal address, it uniquely identifies a single computer on the Internet. Depending on your Internet Service Provider, your computer may be assigned different IP addresses at different times that it connects to them. All Web sites and Web servers also have IP addresses. For example, the IP address of www.frontlinedefenders.org is 217.173.101.253.

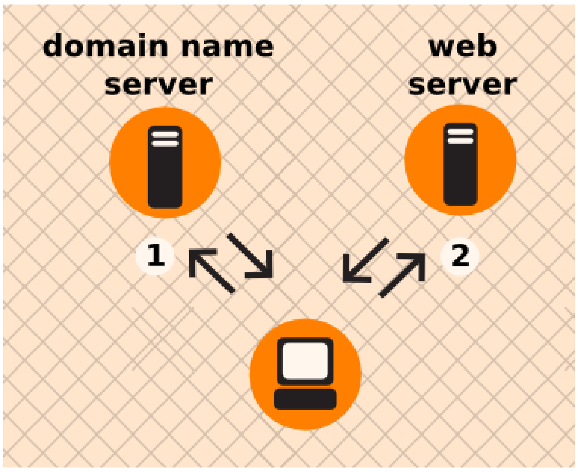
Visiting a Web site

When you want to visit a Web site, you normally type the "name" of the Web site into your browser and not the IP address. For example, to access the Frontline Web site you would type in **`http://www.frontlinedefenders.org`** instead of **`217.173.101.253`**. The name of the Web site is also called the **domain** or **domain name**.

After you type the domain name into the browser, your computer sends a message with this name to the **Domain Name System** (DNS). This system consists of dedicated computers on the Internet that translate names into IP addresses. The DNS means that you need to remember only the Web site's name rather than a complex string of numbers. After the DNS server translates the domain name into an IP address, it shares that information with your computer.

Now your computer can try to connect to the Web site using its IP address. A path from your computer to the destination Web site must be found. This path may travel through countries, oceans and space; it could be thousands of miles long and could pass through numerous computers. How does it know which way to go, when there are hundreds of millions of different Web sites? The task of directing your message to the Web site (and back) is performed by routers, and the process is known as **routing**.

For our purposes, it's worth noting that routers can be given simple instructions on how to behave and can be used as a tool for censorship. Any router can be manipulated to record, re-direct, or block access to certain Web sites.



Example of what happens when you find a Web page:

1. You type in **`http://globalvoicesonline.org/`**. The computer sends the domain name to a selected DNS server (using its numeric address), which sends a message back, containing the IP address for the Global Voices Web site.
2. The browser then sends a request for a connection to that IP address.
3. The request goes through a series of routers until it reaches a router that finds the specific computer needed.
4. This computer sends information back to you, allowing your browser to send the full URL and receive the data to display the page.

Every connection between computers or routers that a message goes through is called a **hop**. The number of hops is the number of computers or routers your message comes in contact with along its way. Below is a sample path taken by a computer to get to www.globalvoicesonline.org. This request passes through at least fourteen computer connections (hops) before reaching its destination.

```
traceroute to globalvoicesonline.org (72.249.186.50), 64 hops max, 40 byte packets
 1  192.168.1.1 (192.168.1.1)  2.425 ms  0.673 ms  0.637 ms
 2  192.168.15.1 (192.168.15.1)  3.824 ms  1.068 ms  1.139 ms
 3  10.92.32.1 (10.92.32.1)  10.712 ms  9.581 ms  98.359 ms
 4  gig-5-3-lbrtnymtn-rtr1.hvc.rr.com (24.164.160.173)  10.720 ms  10.774 ms  11.147 ms
 5  pos-3-1-nycmnya-rtr1.nyc.rr.com (24.164.160.78)  12.533 ms  12.042 ms  11.206 ms
 6  tenge-0-3-0-nwrknjmd-rtr.nyc.rr.com (24.29.97.6)  12.456 ms  13.922 ms  13.821 ms
 7  ae-4-0.cr0.nyc30.tbone.rr.com (66.109.6.78)  15.844 ms  22.984 ms  14.024 ms
 8  ae-1-0.pr0.nyc20.tbone.rr.com (66.109.6.163)  14.605 ms  14.592 ms  43.455 ms
 9  207.88.182.73.ptr.us.xo.net (207.88.182.73)  14.707 ms  14.437 ms  22.936 ms
10  te-4-0-0.rar3.nyc-ny.us.xo.net (207.88.12.26)  24.168 ms  16.683 ms  16.947 ms
11  207.88.14.9.ptr.us.xo.net (207.88.14.9)  45.446 ms  45.360 ms  46.136 ms
12  207.88.14.10.ptr.us.xo.net (207.88.14.10)  70.949 ms  69.782 ms  70.112 ms
13  207.88.185.38.ptr.us.xo.net (207.88.185.38)  70.162 ms  73.824 ms  73.137 ms
14  switch19.rimuhosting.com (65.99.204.18)  70.630 ms  70.344 ms  70.264 ms
15  server1.globalvoicesonline.org (72.249.186.50)  72.347 ms  72.747 ms  74.179 ms
```

Destination reached!

Global Voices aggregates, curates, and amplifies the global conversation online - shining light on places and people other media often ignore. more about us »

Nicaragua: Concerns About Fraud in Recent Elections

If you have used the Internet, you know that normally all of these complex processes are hidden and you don't need to understand them in order to find the information you need. However, when people or organizations attempting to limit your access to information interfere with the operation of the system, your ability to use the Internet may be restricted.

Why This Matters

Censorship can occur at different points in the Internet infrastructure, covering whole domains or subdomains, individual protocols, or specific content identified by filtering software. The best method to avoid censorship will depend on the specific censorship technique used. You may need to understand these differences in order to use the appropriate measures to use the Internet effectively and safely.

Who Controls the Net?

The full story of Internet governance is complicated, political and still being actively disputed. This text is meant to provide enough details to help you understand how certain aspects of the system affect particular methods of restricting access. The key point is that, in some countries, all Internet infrastructure is owned and operated by governments and large regulated telephone companies. A government that wants to block access to information can exercise direct or indirect control over points where that information is produced, or where it enters or exits the country. Governments have extensive legal authority to spy on citizens, and many also go behind what the law allows, using **extra-legal** methods to monitor or restrict Internet use.

Government involvement

The Internet was developed by U.S. government-sponsored research during the 1970s. It gradually spread to academic use, then business and public use. Today, there is a global community of people working to maintain the standards and agreements that attempt to achieve worldwide open connectivity and interoperability.

However, governments are not compelled to implement Internet infrastructure in accordance with these goals or related recommendations about Internet architecture. They can, and some do, design their national telecommunications systems to have single "choke points", places where they can control their whole country's access to specific sites and services, and in some cases prevent access to their section of the Internet from outside. Other governments have passed laws or adopted informal controls to regulate the behavior of private Internet service providers, sometimes compelling them to participate in surveillance or blocking or removing access to particular materials.

Some of the Internet's facilities and coordinating functions are managed by governments or by corporations under government charter. There is no international Internet governance that operates entirely independent from national governments. Governments treat the ability to control Internet and telecommunications infrastructure as matters of national sovereignty, and many have asserted the right to forbid or block access to certain kinds of content and services deemed offensive or dangerous.

Why This Matters

It is important to understand Internet governance in order to relate the sources of Internet censorship to the possible threats. A national government might not only block access to content, but might monitor what information people in its country access, and might penalize users for Internet-related activities that the government deems unacceptable. Governments may both define what to block and may carry out the blocking, or may create legislation, regulations, or extra-legal forces to compel the staff of nominally independent companies to carry out blocking and surveillance. Therefore, depending on a user's situation, attempting to circumvent online censorship can have damaging real-world consequences. When user safety is involved, understanding how Internet is (and is not) controlled is critical.

Filtering Techniques

Internet filtering is a set of techniques that censors use to try to prevent Internet users from accessing particular content or services. Network operators can filter at any point in a network, using a wide variety of technologies, with varying levels of accuracy and customizability. Typically, filtering involves using software to look at what users are attempting to do and to selectively interfere with activities that the operator considers forbidden by policy. A filter could be created and applied by a national government or by a national or local Internet access provider.

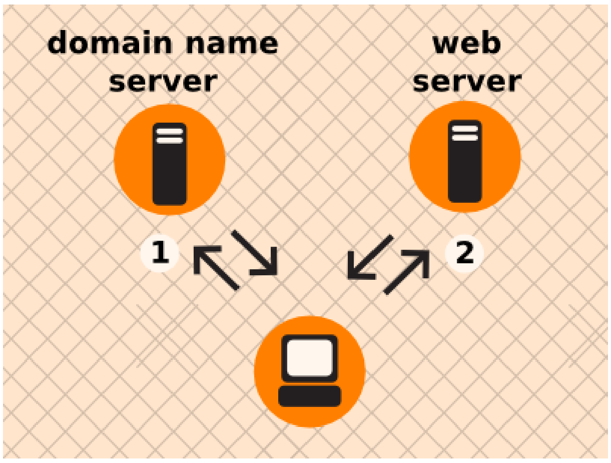
There are four common sorts of filtering you should be aware of.

URL Filtering

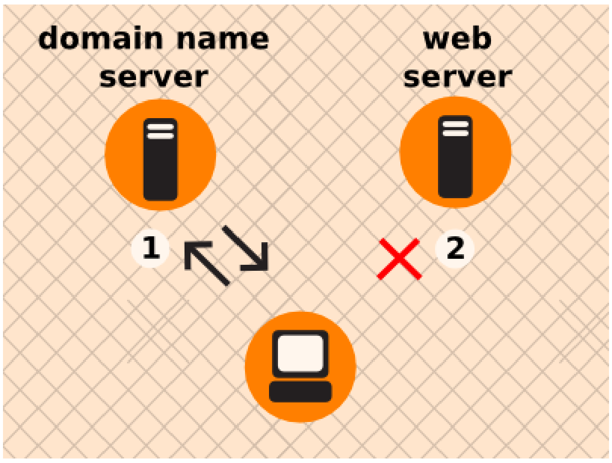
One way for countries and other entities to block access to information on the Web is to prevent access based on the URL -- either the entire URL or some part of it. Internet censors often want to block specific Web domains in their entirety, because they object to the content of those domains. They can block domains either by name or IP number. Sometimes, authorities are more selective, blocking only certain subdomains in a particular domain, while leaving the rest of the domain accessible. For example, they might filter only the subdomain news.bbc.co.uk, while leaving bbc.co.uk and www.bbc.co.uk unfiltered. Similarly, they might want to filter out specific types of content, even if they allow access to the rest of the domain hosting those pages. One way is to look for a directory name, such as "worldservice" to block out BBC foreign language news at bbc.co.uk/worldservice, without affecting the English language Web site. They can even block specific pages based on page names, or search terms in queries, that suggest offensive or undesired content.

DNS Filtering

When people use the Internet to communicate, they generally use domain names such as "somewebsite.com" rather than numeric IP addresses, particularly for Web browsing. However, when computers communicate over the Internet, they require numeric addresses for navigating. When you enter a domain name in a Web browser, the first thing the Web browser does is to ask a DNS (Domain Name System) server, at a known numeric address, to look up the domain name and supply the corresponding IP address.



If the DNS server is configured to block access, it consults a blacklist of banned domain names. When a browser requests the IP address for one of these domain names, the DNS server gives a wrong answer or no answer at all.



Without the IP address, the requesting computer cannot continue, and displays an error message. Since the browser does not get the Web site's IP address, it is not able to contact the site to request a page. The result is to block all pages under a domain name.

Alternatives for circumventing DNS filtering are:

- Access the desired content from another site with a different domain name.
- Asking a different DNS server for the address. This can be done for a single domain or permanently by using a free DNS server or running your own DNS server.
- Finding the numeric address published somewhere.
- Send the query through a different site that is not blocked. E.g, a web proxy or the cache of a search engine.

IP Filtering

When data is sent over the Internet, it is divided into segments and put into packets. A packet contains both the data being sent, and information about how to send it, such as the IP addresses of the computer it came from and the one it should go to. **Routers** are computers that packets pass through on their way from a sender to a receiver, in order to determine where to go next. If censors wants to prevent users from accessing specific servers, they can configure routers that they control to "drop" (not transmit) data destined for IP addresses on a blacklist or to return an error message for them. Filtering based solely on IP addresses blocks *all* services provided by a particular server, such as both Web sites and e-mail servers. Since only the IP address is inspected, multiple **domain names** that share the same IP address are also blocked, even if only one is prohibited.

To circumvent IP filtering, it may be possible to access the desired content elsewhere, or to route requests through sites not subject to blocking.

Port blocking

Ports are like numbered doors in a building, each leading to a different room or suite. On a computer, ports are also numbered: the well-known standard port numbers are from 0 to 1024, but others can go up to 65535. Each numbered port normally offers a specific service (for example, web access or e-mail) on a server or PC. When one computer requests access to a particular type of service on another computer, it specifies a port number for the request. The computer providing the service "listens" for requests that use a particular port number.

Blacklisting individual port numbers restricts access to individual services on a server, such as Web or e-mail. Common services on the Internet have characteristic port numbers. The relationships between services and port numbers are assigned by **IANA**, but are not mandatory. These assignments allow routers to make a guess as to the service being accessed. Thus, to block just the web traffic to a site, a censor might block only port 80, because that is the port typically used for web access.

The most direct method for circumventing port blocking is to use non-standard ports to provide standard services. Users must have some system knowledge to take advantage of this, in order to configure Web browsers or e-mail clients to use the non-standard ports. Other methods of accessing the content include accessing the same or similar services on other cooperating servers, or accessing the blocked servers through a non-blocked location.

Why This Matters

These censorship techniques depend on the working of different parts of the Internet structure described above. You should have some understanding of whichever of them applies in your situation. If you wish to create an unblocked server outside the location doing the blocking, you will need more detailed information.

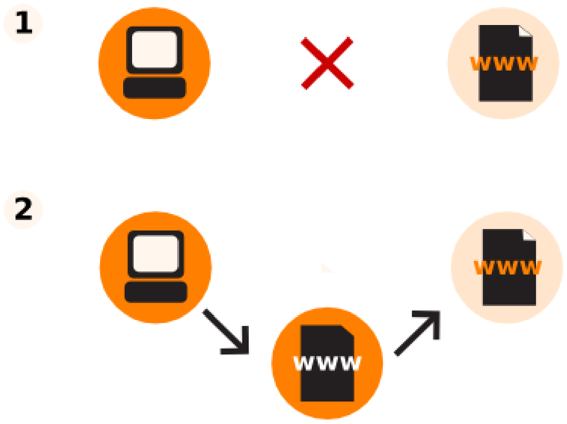
Simple Tricks

There are a number of techniques to get past Internet filtering. If your aim is simply to reach pages or services on the Internet that are blocked from your location, and you are not concerned whether other people can detect and monitor your circumvention, these techniques may be all you need:

- Using third-party Web sites to reach blocked content.
- Using alternative domain names (or domain name servers) to reach blocked content.
- Using e-mail gateways to retrieve blocked Web pages over e-mail.

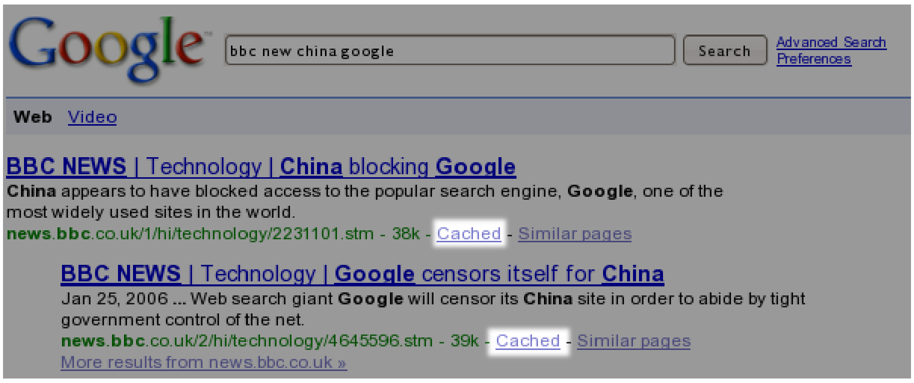
Using third-party sites

There are a number of different ways you can reach the content on a Web page by going through a third-party web site rather than directly to the source web site.



Cached Pages

Many search engines keep copies of Web pages they have previously indexed, called **cached** pages. When searching for a Web site, look for a small link labeled "cached" next to your search results. Since you are retrieving a copy of the blocked page from the search engine's servers, and not from the blocked Web site itself, you may be able to access the blocked content. However, some countries have targeted caching services for blocking, as well.



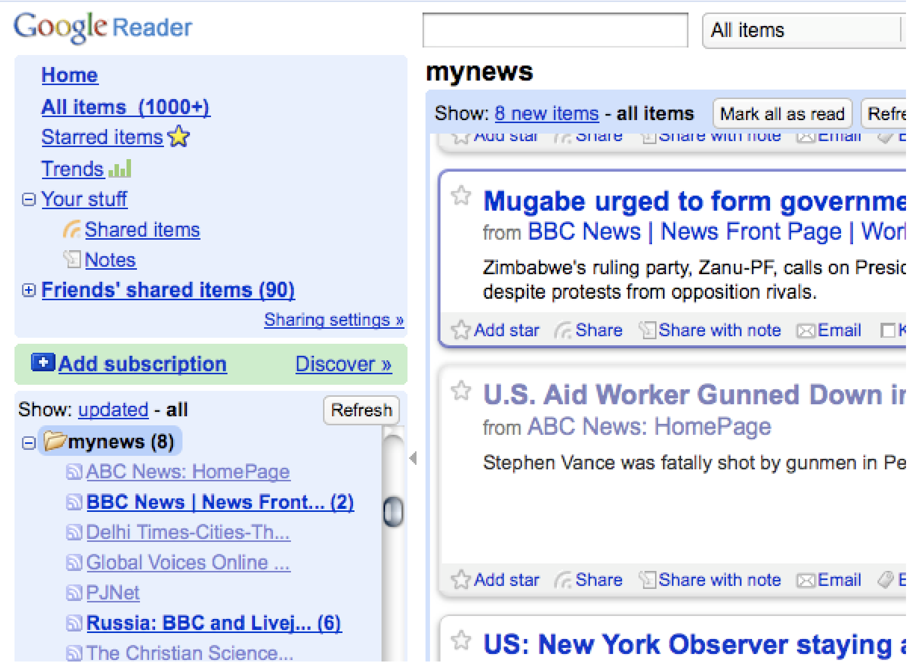
BBC NEWS | Technology | China blocking Google
China appears to have blocked access to the popular search engine, **Google**, one of the most widely used sites in the world.
news.bbc.co.uk/1/hi/technology/2231101.stm - 38k - Cached - Similar pages

BBC NEWS | Technology | Google censors itself for China
Jan 25, 2006 ... Web search giant **Google** will censor its **China** site in order to abide by tight government control of the net.
news.bbc.co.uk/2/hi/technology/4645596.stm - 39k - Cached - Similar pages
More results from news.bbc.co.uk »

RSS Aggregators

RSS aggregators are Web sites that allow you to subscribe to and read **RSS feeds**, which are streams of news or other information put out by sites you have chosen. (RSS stands for "Really Simple Syndication"; for more on how to use it, see http://rssexplained.blogspot.com/.) An RSS aggregator connects to Web sites, downloads the feeds that you have selected, and displays them. Since it is the aggregator connecting to the Web sites, and not you, you may be able to access sites that would otherwise be blocked. This technique works only for Web sites that publish RSS feeds of their content, of course, and therefore is most useful for blogs and news sites. There are a lot of free, online RSS aggregators available. Some of the most popular ones include Google Reader (http://reader.google.com) and Bloglines (http://www.bloglines.com).

Below is an example of Google Reader displaying the news:



Mugabe urged to form governme
from BBC News | News Front Page | Worl
Zimbabwe's ruling party, Zanu-PF, calls on Presic
despite protests from opposition rivals.

U.S. Aid Worker Gunned Down ir
from ABC News: HomePage
Stephen Vance was fatally shot by gunmen in Pe

US: New York Observer staying a

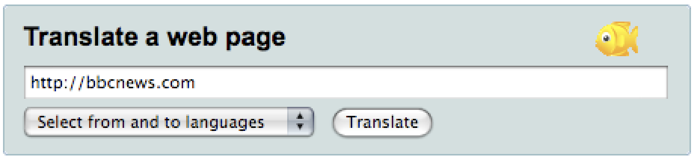
Translators

There are many language translation services available on the Internet, often provided by search engines. If you access a Web site through a translation service, the translation service is accessing the blocked site, not you. This allows you to read the blocked content translated into a number of different languages.

You can use the translation service to bypass blocking, even if you don't actually need to translate the text. You do this by choosing translation from a language that does not appear on the original Web site back to the original language. For example, to use a translation service to view an English-language Web site, choose translation from Chinese to English. The translation service translates only the Chinese sections (there are none), and leaves the English sections (which is the whole Web page) untranslated.

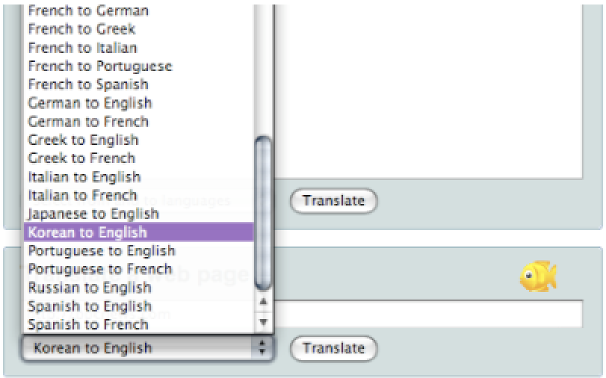
Popular translation services include http://babelfish.yahoo.com/ and http://translate.google.com/.

The example below illustrates the three steps necessary to view a page in Babelfish. First, enter the URL of the Web site you wish to visit:

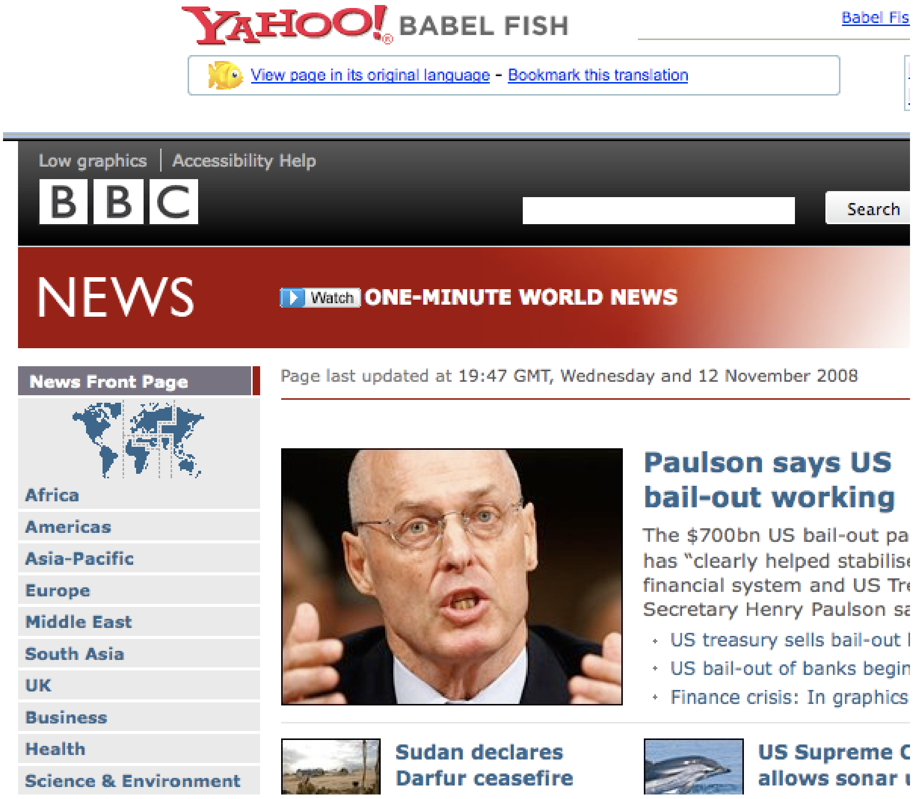


http://bbcnews.com

Next, choose the language you wish to read the Web site in. In this example, we tell Babelfish to translate from Korean to English. Since there is no Korean text, the page will remain untranslated.



When you have chosen the language, click "Translate" and the page displays.



Page last updated at 19:47 GMT, Wednesday and 12 November 2008

Paulson says US bail-out working

The $700bn US bail-out pa has "clearly helped stabilise financial system and US Tre Secretary Henry Paulson sa

- US treasury sells bail-out l
- US bail-out of banks begin
- Finance crisis: In graphics

Sudan declares Darfur ceasefire

US Supreme C allows sonar u

Low-Bandwidth Filters

Low-bandwidth filters are Web services designed to make browsing the Web easier in places where connection speeds are slow. They remove or reduce images, remove advertisements, and otherwise compress the Web site to make it use less data, so it downloads faster. But, as with translation and aggregation services, you can also use low-bandwidth filters to bypass simple Web site blocking by fetching Web sites from their servers rather than from your computer. One useful low-bandwidth filter is at http://loband.org/.

Using Alternative Domain Servers or Names

Simply speaking, a DNS server translates a human-friendly Web address such as google.com into the IP address that identifies the specific server with that page on the Internet, such as 72.14.207.19. This service is most often provided by DNS servers maintained by your Internet Service Provider (**ISP**). Simple DNS blocking is implemented by giving an incorrect or invalid response to a DNS request.

You can potentially bypass this type of blocking with these techniques:

Alternate Domain Names

One of the most common ways to censor a Web site is to block access to its domain name, for example, "news.bbc.co.uk". However, sites are often accessible at other domain names, such as "newsrss.bbc.co.uk". If one domain name is blocked, try to see if the content is available at another domain.

Alternative DNS Servers

An extension of this technique is to bypass the Domain Name Servers of your local ISP, using third-party servers to reach domains that may be blocked by the ISP's servers. There are a number of free, internationally available DNS services that you can try. OpenDNS (https://www.opendns.com/) provides one such service and also maintains guides on how to change the DNS server that your computer uses (https://www.opendns.com/smb/start/computer/). There is also an updated list of available DNS servers from around the world at http://www.dnsserverlist.org/.

Using e-mail services

E-mail and Web-mail services can be used to share documents with groups of friends or colleagues, and even to browse the Web.

Accessing web pages through e-mail

Similar to low-bandwidth filters, there are services intended for people with slow or unreliable Internet connections that let you request a Web page via e-mail. The service sends a reply e-mail that includes the requested Web page either in the body of the message or as an attachment. These services can be quite cumbersome to use, since they require you to send a separate request for one or more Web pages, and then wait for the reply, but, in certain situations, they can be very effective at reaching blocked Web pages, especially if you use them from a secure Web mail service.

One such service is pagegetter.com. To use it, send an e-mail, including one or more URLs in the subject or body of your message, to web@pagegetter.com. You automatically receive the full requested web page, complete with embedded graphics.

Web pages with **frames** will be sent in multiple e-mails, because many e-mail clients cannot display frames. (Frames are a way of showing multiple pages on a single screen.) But if your e-mail client supports frames (for example, Outlook Express) you can receive all frames in a single message. In this case, send the e-mail to frames@pagegetter.com.

To receive a text-only version of the requested page, write instead to text@pagegetter.com. This is especially useful for Personal Digital Assistants (PDAs), cell phones, and text-only e-mail systems. You can also send an e-mail to HTML@pagegetter.com to receive the full HTML page with no graphics.

A similar service is found at **web2mail.com.** To use it, send an e-mail message to www@web2mail.com with the Web address (URL) of the Web page you want in the Subject line. You can also perform simple Web searches by typing searches into the Subject line. For example you can search for censorship circumvention tools by typing "search censorship circumvention tools" in the subject of an e-mail message and sending it to www@web2mail.com.

You can find more information and support on this topic on the ACCMAIL mailing list. To subscribe, send an e-mail with "SUBSCRIBE ACCMAIL" in the body to listserv@listserv.aol.com.

Using Web mail to share documents

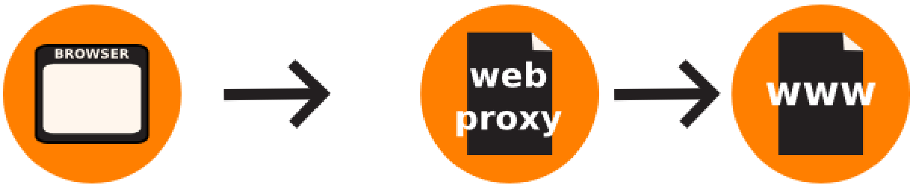
If you are trying to share documents online, but want to control who can see them, you can keep them in a private space where they are visible only to those with the correct password. A simple way to share documents among a small group of friends or colleagues is to use a single Web mail account with an online e-mail provider, such as Gmail (https://mail.google.com/), and to share the user name and password with those who need to access the documents. Since most Web mail providers are free, it is easy to switch to a new account at intervals, making it harder for anyone outside the group to keep track of what you are doing. A list of free online e-mail providers is located at www.emailaddresses.com/email_web.htm.

Advantages and Risks

These simple techniques are quick and easy to use; you can try them with minimal effort. Many of them will work at least some of the time in many situations. However, they are also easy to detect and block. Since they do not encrypt or otherwise hide your communications, they are also vulnerable to keyword-based blocking and monitoring.

What is a Web Proxy?

A Web proxy allows you to retrieve a Web site even when direct access to that site is blocked at your location. Typically, a Web proxy features a form where you submit the URL of a site that you want to view. The proxy then shows you the page, but prevents a direct connection between you and the requested Web site.



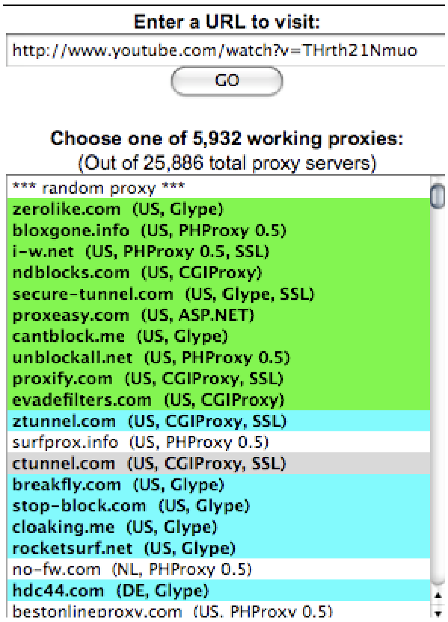
When using a Web proxy, you do not have to install software or change settings on your computer. Instead, you go to the URL of the Web proxy, then enter the URL you wish to visit, and click the "submit" button (or equivalent). A Web proxy can be used from any computer, including those in Internet cafÃ©s.

Examples of free Web proxies include **CGIProxy**, **PHProxy** and **Zelune**. All of them provide the same basic functionality, but some are better at providing certain functions, such as access to videos. These and other Web proxy programs, like **Glype**, **Psiphon**, **Picidae** and **bblocked**, are software programs that may be run on many different computers.

You can find lists of Web proxies on sites like http://www.proxy.org/, by joining the mailing list at http://www.peacefire.org/circumventor/, or just by searching for "free Web proxy" in any search engine.

(If you are in a country with unrestricted Internet access and you are willing to help others get around censorship, you can install a Web proxy script on your own Web site or on your home computer.)

Proxy.org lists literally thousands of free Web proxies:



Enter a URL to visit:

http://www.youtube.com/watch?v=THrth21Nmuo

Choose one of 5,932 working proxies:
(Out of 25,886 total proxy servers)

*** random proxy ***
zerolike.com (US, Glype)
bloxgone.info (US, PHProxy 0.5)
i-w.net (US, PHProxy 0.5, SSL)
ndblocks.com (US, CGIProxy)
secure-tunnel.com (US, Glype, SSL)
proxeasy.com (US, ASP.NET)
cantblock.me (US, Glype)
unblockall.net (US, PHProxy 0.5)
proxify.com (US, CGIProxy, SSL)
evadefilters.com (US, CGIProxy)
ztunnel.com (US, CGIProxy, SSL)
surfprox.info (US, PHProxy 0.5)
ctunnel.com (US, CGIProxy, SSL)
breakfly.com (US, Glype)
stop-block.com (US, Glype)
cloaking.me (US, Glype)
rocketsurf.net (US, Glype)
no-fw.com (NL, PHProxy 0.5)
hdc44.com (DE, Glype)
bestonlineproxy.com (US, PHProxy 0.5)

There are also private Web proxies. These are usually known only to a small group of contacts of the individual running the proxy. They may be useful in special circumstances, when you need to be sure to be able to access specific types of content or need the privacy offered by a proxy operated by someone you trust.

Advantages and Risks

Web proxies are easy to use -- you don't need to install any software, you can use a public Web proxy even if you don't have a trusted contact in an unfiltered location. Private Web proxies can be customized to meet the specific needs of users and are less likely to be discovered and blocked by any filtering authorities.

But Web proxies have potential disadvantages. They often allow only Web traffic (HTTP), so they can't be used for other services such as e-mail or instant messaging. Many cannot use multimedia (such as YouTube) or be used with encryption (SSL). Web services that require authentication (such as Web-based e-mail) may not be fully functional through Web proxies or may make you vulnerable to having your passwords or other information monitored or stolen.

Web proxies also can be blocked or intercepted. The addresses of public Web proxies are generally well known and access to them may be blocked. Private Web proxies require that a user have a contact in an unfiltered location. Unencrypted communications with Web proxies can be intercepted by network operators, thus keyword filtering may still work against unencrypted Web proxies.

Web proxy users also need to keep in mind that the operators of their Web proxies can read their communications and record the IP address from which the Web proxy was used. If that information would put you at risk, you should consider your choice of proxy carefully.

Using PHProxy

PHProxy is a free **Web proxy** that provides access to Web sites that would otherwise be blocked.

PHProxy was written in the **PHP** programming language, originally by someone using the name Abdullah Arif, who stopped working on the project in 2007. Nonetheless, it remains functional and useful and many people have used it to set up their own public Web proxies.

Where can I access PHProxy?

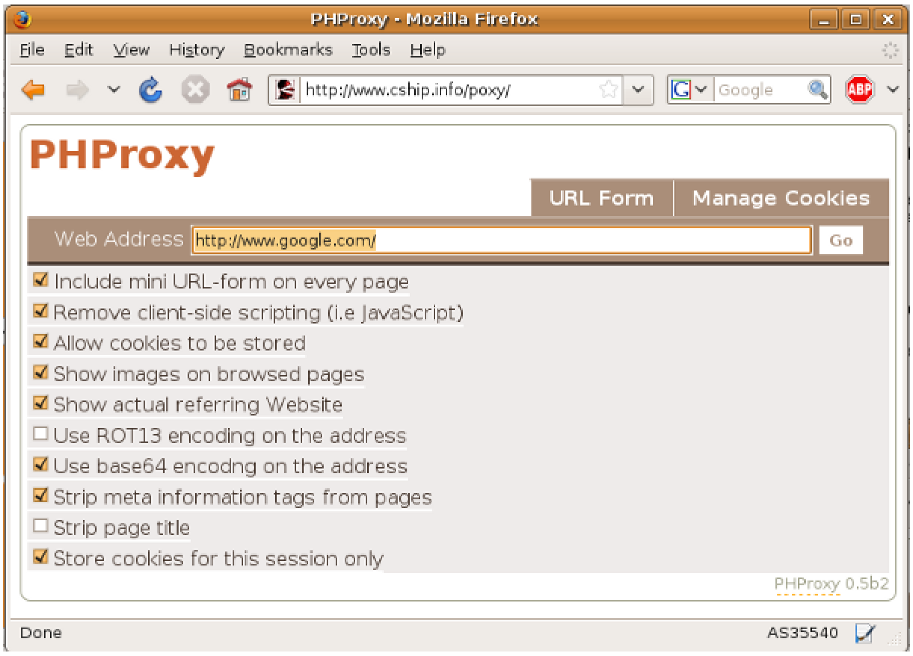
You can find a public PHProxy service by searching for "PHProxy" in any search engine, but someone you know who has space on a Web server with unrestricted Internet access can also set up a custom PHProxy service for you.

(If you have space on a Web server with unrestricted Internet access, you can set up a PHProxy service yourself for use by people whose access is restricted. To do so, you can download the PHProxy script at http://sourceforge.net/projects/poxy/.)

How does it work?

Here's an example that illustrates how PHProxy works:

1. Enter the address of the PHProxy service, for example http://www.cship.info/poxy/ , in your Web browser.
2. In the "Web Address" box on the PHProxy page, enter the address of the Web site you want to visit, for example, http://www.google.com. You can keep the default options.
3. Click "Go" or press Enter.

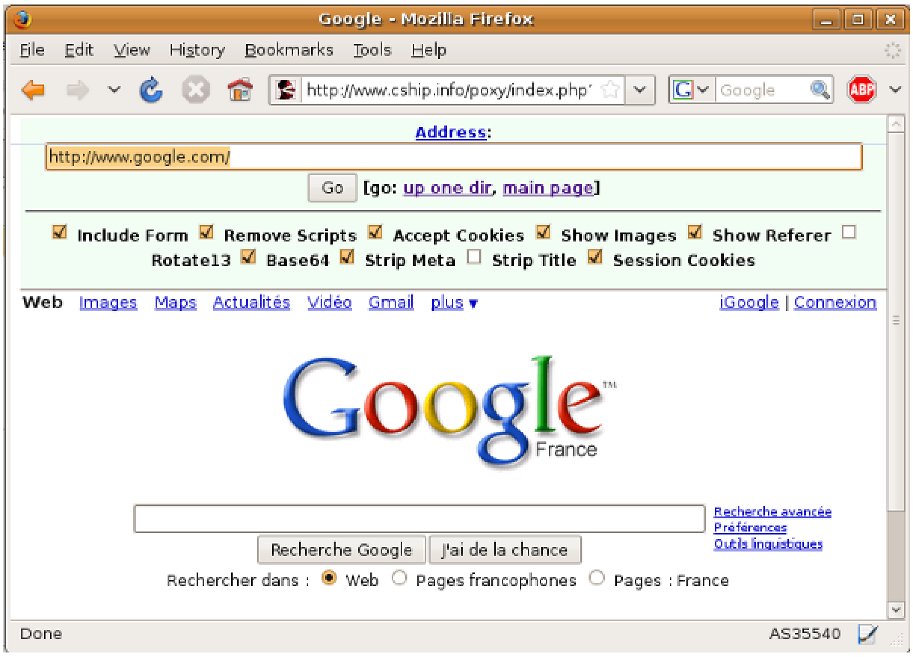


PHProxy - Mozilla Firefox
File Edit View History Bookmarks Tools Help
http://www.cship.info/poxy/
Google
PHProxy
URL Form
Manage Cookies
Go
PHProxy 0.5b2
Done
AS35540

Web Address http://www.google.com/

☑ Include mini URL-form on every page
☑ Remove client-side scripting (i.e JavaScript)
☑ Allow cookies to be stored
☑ Show images on browsed pages
☑ Show actual referring Website
□ Use ROT13 encoding on the address
☑ Use base64 encodng on the address
☑ Strip meta information tags from pages
□ Strip page title
☑ Store cookies for this session only

The Web site you wanted to visit is displayed in the browser window.



http://www.cship.info/poxy/index.php'

Address: http://www.google.com/

Go [go: up one dir, main page]

☑ Include Form ☑ Remove Scripts ☑ Accept Cookies ☑ Show Images ☑ Show Referer □ Rotate13 ☑ Base64 ☑ Strip Meta □ Strip Title ☑ Session Cookies

Rechercher dans : ● Web ○ Pages francophones ○ Pages : France

To continue browsing, you can either:

- Click any link. The Web proxy is automatically used to retrieve linked pages.
- Enter a new URL in the "Address" box at the top of the page.

Advanced options

Usually, you can keep the default options to browse. However you can choose between several advanced options:

- **Include mini URL-form on every page:** Check this option if you want to have a form on the proxified Web sites so you can enter new URLs without going back to the startpage of the PHProxy. If you only have a small screen you may want to de-select this option so you have more space for the target Web page.

- **Remove client-side scripting (i.e., JavaScript):** JavaScript is a technology required by some modern Web sites (like Web mail services). Sometimes JavaScript can be unwanted because it is also used to deliver advertisements or even to discover your identity.

- **Allow cookies to be stored:** Cookies are little text files with a distinct user ID which are normally automatically stored by your browser. They are required for some websites which need authentication but can be used to track your identity. With this option turned on every cookie is stored for a long time. If you want to allow cookies for this session only, de-select this option and select "Store cookies for this session only" (see below).

- **Show images on browsed pages:** If you are on a slow Internet connection, you can de-select this option so the Web sites load faster.

- **Show actual referring Website:** By default your browser sends every website the URL you are coming from. For example if you search on Google for "Internet censorship wiki" the results page will be http://www.google.com/search?q=internet+censorship+wiki. When you then click on the link http://en.cship.org/wiki/ from the results that website will get the Google link which can be stored in logfiles and analysed automatically. For better anonymity you can de-select this option. Some websites may not work if this option is de-selected.

- **Use ROT13/base64 encoding:** This option will change the way the URL of the Web site you want to visit is transfered. For example, the URL http://en.cship.org/wiki/ will be uggc://ra.pfuvc.bet/jvxv/ in ROT13 and aHR0cDovL2VuLmNzaGlwLm9yZy93aWtpL01haW5fUGFnZQ in base64. Both encoding techniques are well known, so they can not be considered as encryption at all. Still, they can be used to confuse simple keyword filters. If you use SSL encryption (the URL of the PHProxy starts with https) this encoding would be redundant, since the connection is already encrypted properly and hidden from filters.

- **Strip meta information tags from pages:** Meta tags are additional information stored in many websites to be used automatically by computer programs. Such information may include name of the author, description of the site content or keywords for search engines. You may check this option to avoid presenting this information to keyword filters.

- **Strip page title:** With this option turned on, PHProxy deletes the page title of the website, which you normally see in the title bar on top of your browser. This can be useful, for example, to hide the name of the Web site you are visiting when you minimize your browser.

- **Store cookies for this session only:** Similar to the "Allow cookies to be stored" option. With this option turned on, your cookies are only stored until you close your PHProxy session.

Using psiphon

psiphon is a **Web proxy** designed to be used between people who have pre-existing private, trusted relationships (such as friends and family). A person in an unrestricted location provides a psiphon **proxy service** to a person they know in a location where access is limited. It is not intended to be a public, open proxy service.

If you want to use psiphon to bypass Internet restrictions, you first need to find someone in a location with no Internet restrictions who is willing to provide a psiphon **node** for you. There is an official psiphon forum at http://psiphon.civisec.org/forum/ where psiphon users share information about available psiphon nodes. You may be able to find a trustworthy person through that forum, but note that the person whose psiphon node you use will have access to all of your Internet activity, *including passwords and other private data*.

(If you have a server or Web space in a location with no Internet restrictions, you can install psiphon for other people to use. Visit http://psiphon.ca/download.php for more information.)

Connecting to a psiphon Proxy

When you have established contact with the owner of a psiphon node, that person will send you information that may look like this:

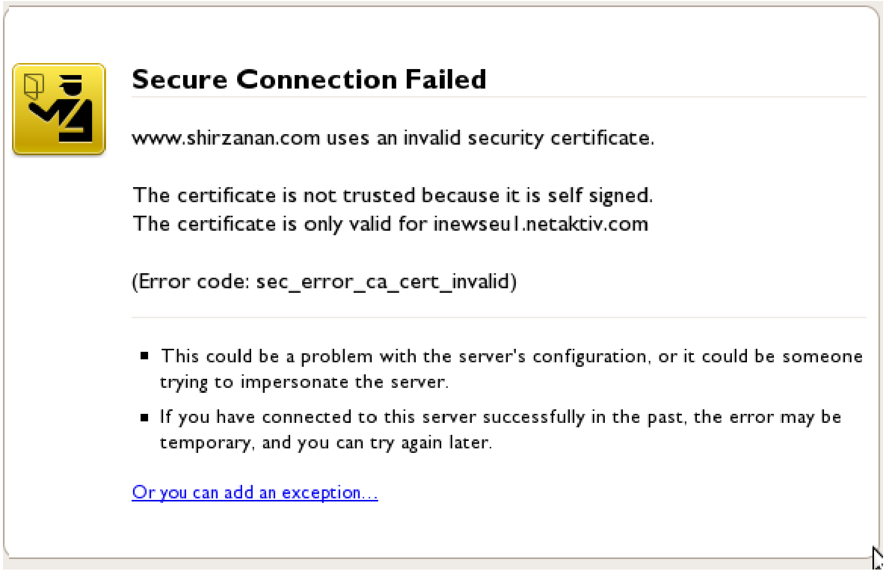
URL: https://86.103.195.150:443/cship/
Username: cship
Password: cship

To use the psiphon proxy, enter the **URL** you receive into your Web browser and then sign in with the appropriate account information.

Adding an SSL Exception

The first time that you connect to a psiphon URL, your Web browser might show an error message about a non-valid SSL certificate, as shown below. This happens because you are using an **SSL** connection (indicated by "https:" in the URL), and SSL connections are normally supposed to be secured with official SSL certificates to authenticate the server. Official SSL certificates cost money, so the owner of the psiphon node might not have one (so far, most psiphon nodes don't have them). Ignoring this error message *may pose a risk to your privacy* because a clever network operator could pretend to be the psiphon server. If you are concerned primarily with access and not privacy, ignoring this error could be appropriate.

If you choose to proceed, you can add an exception rule in your browser so that you will not see it every time you connect. In this example, the exception is added to the **Firefox** 3 browser:



Secure Connection Failed

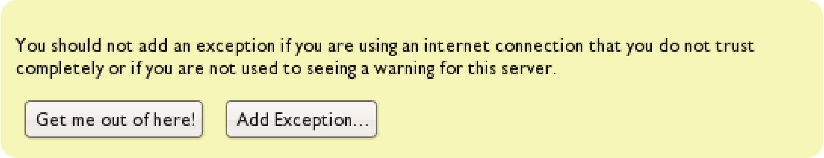
www.shirzanan.com uses an invalid security certificate.

The certificate is not trusted because it is self signed.
The certificate is only valid for inewseu1.netaktiv.com

(Error code: sec_error_ca_cert_invalid)

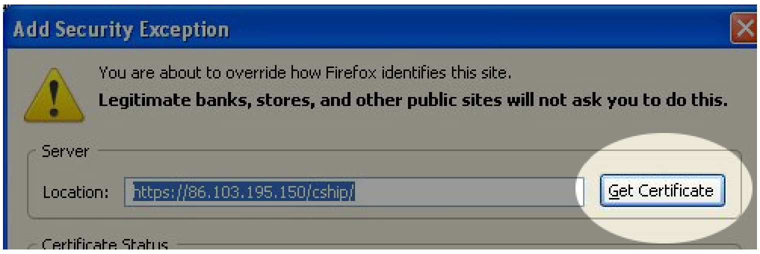
- This could be a problem with the server's configuration, or it could be someone trying to impersonate the server.
- If you have connected to this server successfully in the past, the error may be temporary, and you can try again later.

- Click the "Or you can add an exception" link at the bottom of the page. The browser displays more information and buttons.



You should not add an exception if you are using an internet connection that you do not trust completely or if you are not used to seeing a warning for this server.

- Click "Add Exception". The browser opens a dialog box, with the URL you originally entered in the Location box:



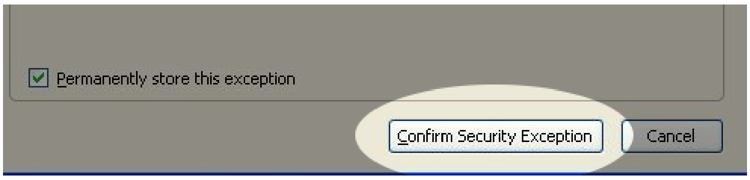
Add Security Exception

You are about to override how Firefox identifies this site.
Legitimate banks, stores, and other public sites will not ask you to do this.

Server

Location: https://86.103.195.150/cship/

- Click "Get Certificate". More information appears in the dialog box.



☑ Permanently store this exception

- Click "Confirm Security Exception."

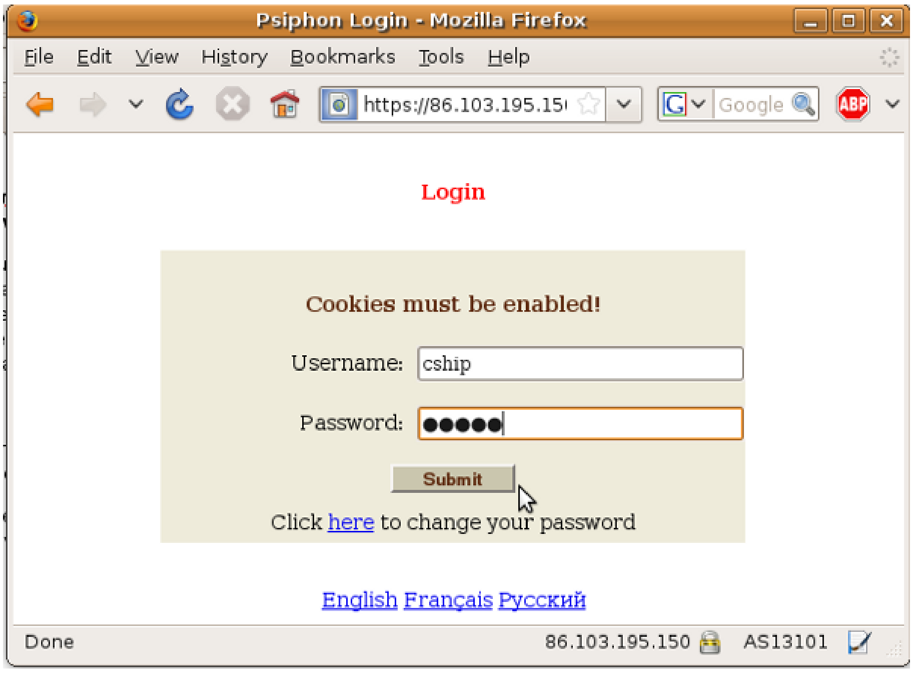
If you're concerned about privacy

Adding a security exception or ignoring the security warning, as described above, creates some risk for privacy because a clever eavesdropper who controls part of your network connection could try to trick you by pretending to be a psiphon server. The severity of this risk depends on how likely it is that someone will try to intercept your communications in this way. In some environments, ignoring the security warning once may not be a substantial risk. (If the first connection wasn't tampered with, subsequent connections will be safe because Firefox remembers the identity of the site you communicated with.) If you're concerned primarily with circumvention and not with privacy, this concern may not be relevant to you.

If you're specifically concerned about privacy and preventing eavesdropping, there are safer ways to verify a site's identity before adding a security exception. One way that may work with Firefox is to use the **Perspectives** software from Carnegie Mellon University (http://www.cs.cmu.edu/~perspectives/). Perspectives confirms that a psiphon site, or other Web site without an official security certificate, looks the same to you as it does to several other servers.

Logging in to the Proxy

When you see the login page, enter the username and password you got from your contact (in this example both are "cship"). Make sure that the URL starts with "https" so that you are using the psiphon node over a secure encrypted connection.


Psiphon Login - Mozilla Firefox
File Edit View History Bookmarks Tools Help
https://86.103.195.15
Google

Login

Cookies must be enabled!

Username: cship

Password: ●●●●●

Submit

Click here to change your password

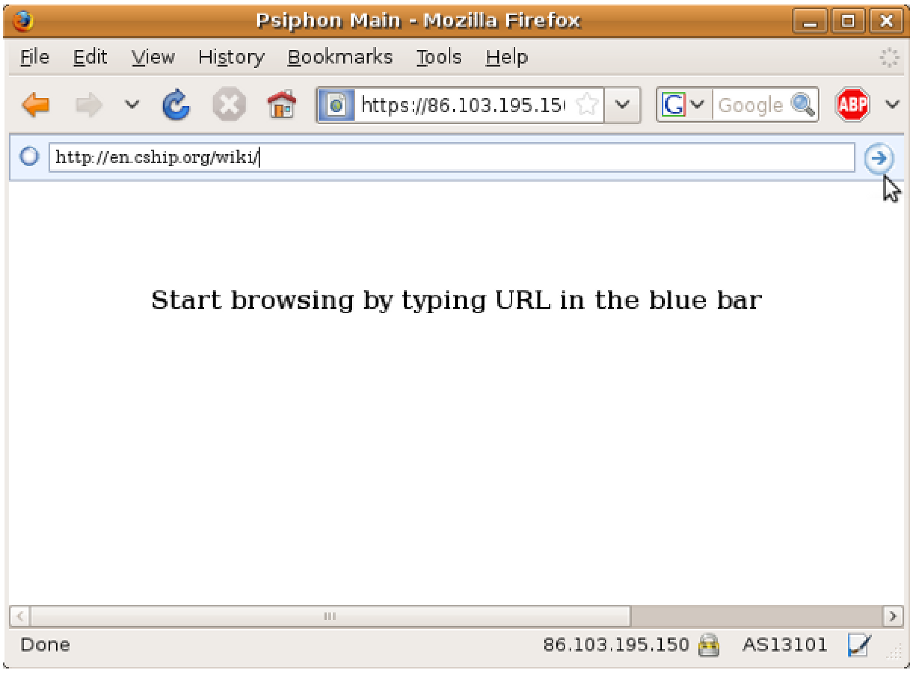
English Français Русский

Done
86.103.195.150
AS13101

Browsing via the Proxy

After you login, you will see a psiphon start page.

Enter the URL for the Web site you want to visit (in this example, http://en.cship.org/wiki/), in the box at the top of the page (under the address box for the browser itself).



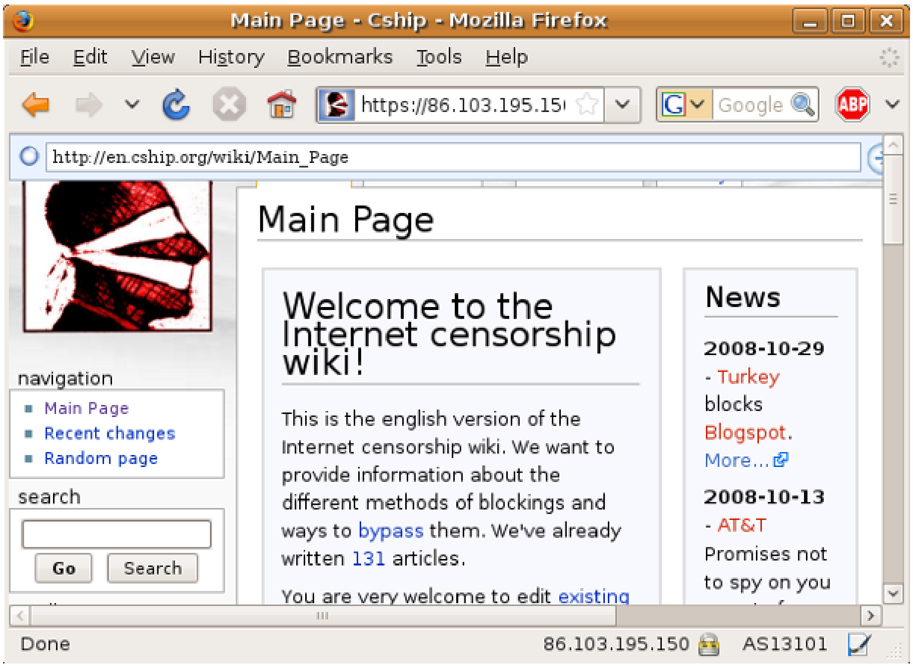
Psiphon Main - Mozilla Firefox
File Edit View History Bookmarks Tools Help
https://86.103.195.15
Google
ABP
http://en.cship.org/wiki/
Done
86.103.195.150
AS13101

Start browsing by typing URL in the blue bar

Click the arrow button on the screen or press the Enter key on your keyboard. The browser displays the Web site whose URL you entered, with the psiphon address box at the top.

To continue browsing you can either:

- Click any link. The Web proxy is automatically used to retrieve linked pages.
- Enter a new URL in the psiphon address box at the top of the page (*not* the browser's address box).



Main Page

Welcome to the Internet censorship wiki!

This is the english version of the Internet censorship wiki. We want to provide information about the different methods of blockings and ways to bypass them. We've already written 131 articles.

You are very welcome to edit existing

News

2008-10-29 - Turkey blocks Blogspot. More...

2008-10-13 - AT&T Promises not to spy on you

Keep in mind that the owner of the psiphon node can monitor and log every Web site and even every password you transfer over that node. In fact, psiphon normally displays a list of the URLs being viewed to the psiphonode operator. That is why it is important that your contact is someone you trust.

Using psiphon 2

psiphon2 is a special kind of webproxy which works unlike other webproxies (like CGIProxy or PHProxy) with an authentication. To use psiphon2 you need the URL (address) and a account (username and password). This makes the use a little more difficult, but adds a lot of security.

How to get a psiphon2 account

To prevent and monitor the blocking of a psiphon2 node we work with a "web of trust", so you need an invitation from a user who already has a psiphon2 account.

Use an invitation link to register

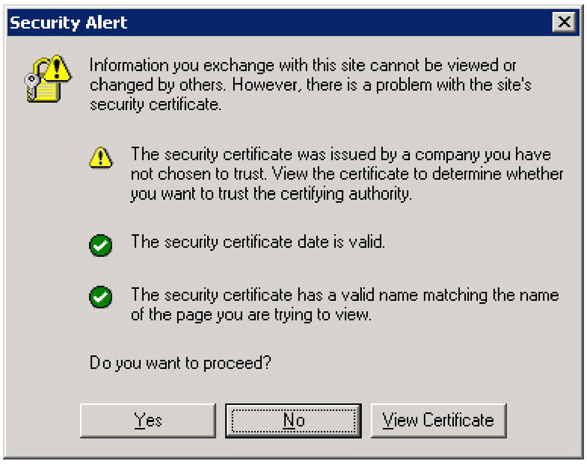
Once you got an invitation link like "https://85.31.189.76/w.php?p=384BC" access that website with your favorite web browser (for example Firefox or Internet Explorer).

Accept the SSL error message

When you access the website for the first time you will see an error message because of the invalid SSL certificate. SSL certificates are used to guarantee the identity of a server. A SSL certificate signed by a large Certificate authority costs a lot of money, so it would be too expensive to buy such a certificate for every psiphon2 node. Nevertheless the connection is completely encrypted and you can safely confirm the error message.

SSL-Error with Internet Explorer 6

If you use Internet Explorer 6, the error message will look like this:



Information you exchange with this site cannot be viewed or changed by others. However, there is a problem with the site's security certificate.

The security certificate was issued by a company you have not chosen to trust. View the certificate to determine whether you want to trust the certifying authority.

The security certificate date is valid.

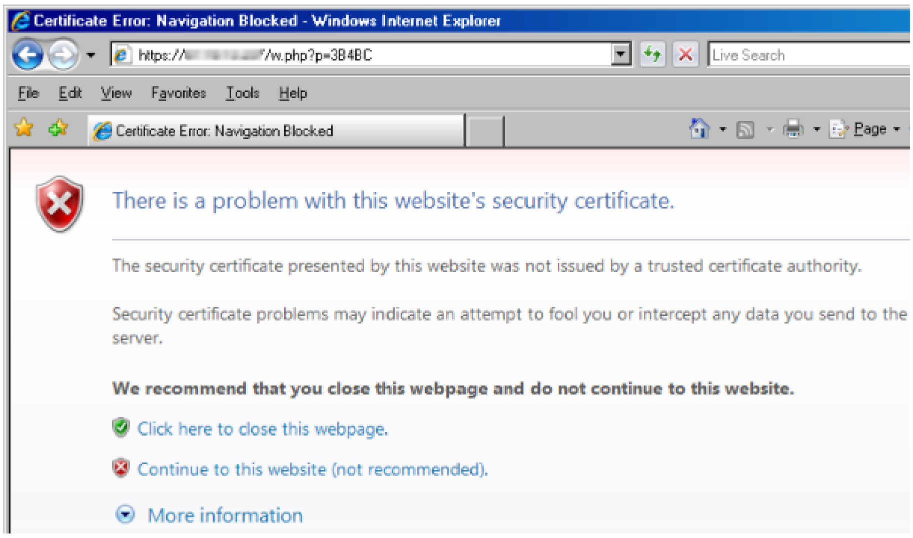
The security certificate has a valid name matching the name of the page you are trying to view.

Do you want to proceed?

Please confirm the message with a click on "Yes".

SSL-Error with Internet Explorer 7

If you use Internet Explorer 7, the error message will look like this:


Certificate Error: Navigation Blocked - Windows Internet Explorer
https://[redacted]/w.php?p=3B4BC
Live Search
File
Edit
View
Favorites
Tools
Help
Certificate Error: Navigation Blocked
Page

There is a problem with this website's security certificate.

The security certificate presented by this website was not issued by a trusted certificate authority.

Security certificate problems may indicate an attempt to fool you or intercept any data you send to the server.

We recommend that you close this webpage and do not continue to this website.

Click here to close this webpage.

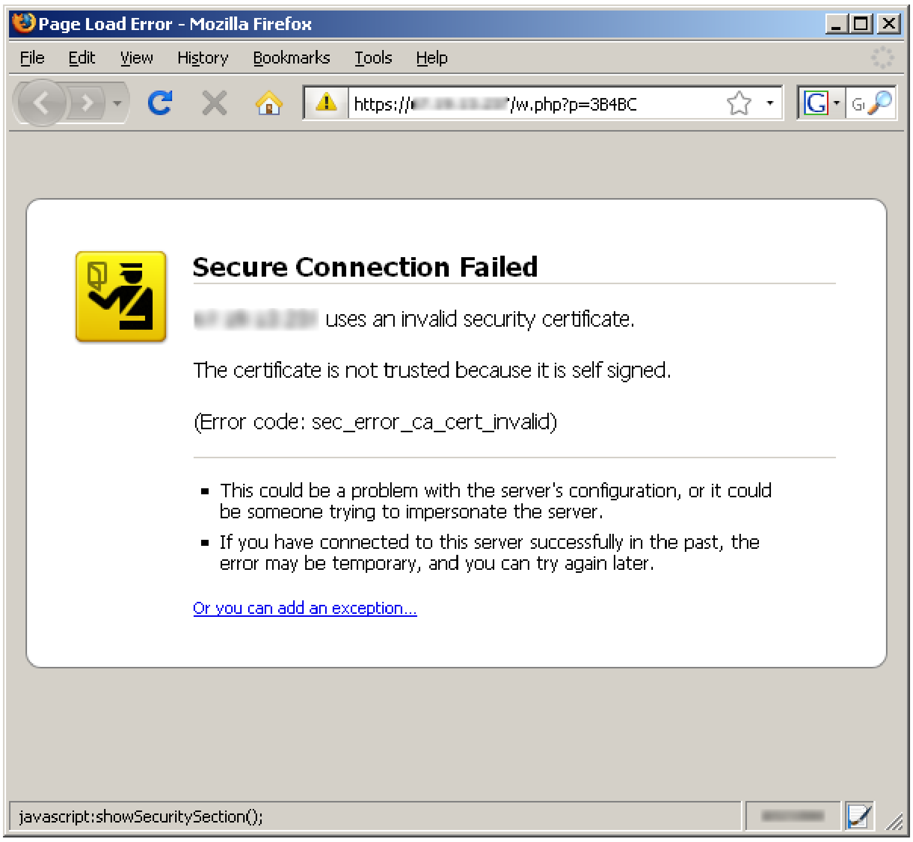
Continue to this website (not recommended).

More information

Please confirm it with a click on "Continue to this website (not recommended)."

SSL-Error with Firefox 3

If you use the Firefox 3 browser it is a little more complicated:


Page Load Error - Mozilla Firefox
File
Edit
View
History
Bookmarks
Tools
Help
https://[redacted]/w.php?p=3B4BC

Secure Connection Failed

[redacted] uses an invalid security certificate.

The certificate is not trusted because it is self signed.

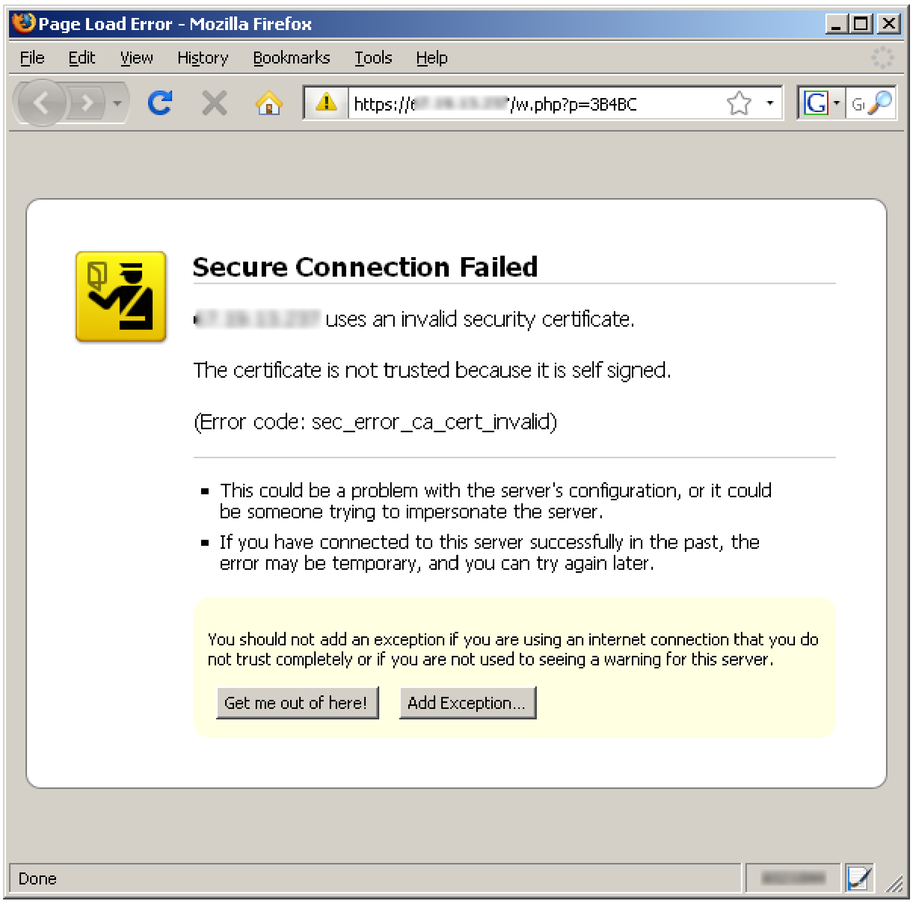
(Error code: sec_error_ca_cert_invalid)

- This could be a problem with the server's configuration, or it could be someone trying to impersonate the server.
- If you have connected to this server successfully in the past, the error may be temporary, and you can try again later.

Or you can add an exception…

javascript:showSecuritySection();

First click on "Or you can add an exception..."


Page Load Error - Mozilla Firefox
File
Edit
View
History
Bookmarks
Tools
Help
https://[redacted]/w.php?p=3B4BC
Done

Secure Connection Failed

[redacted] uses an invalid security certificate.

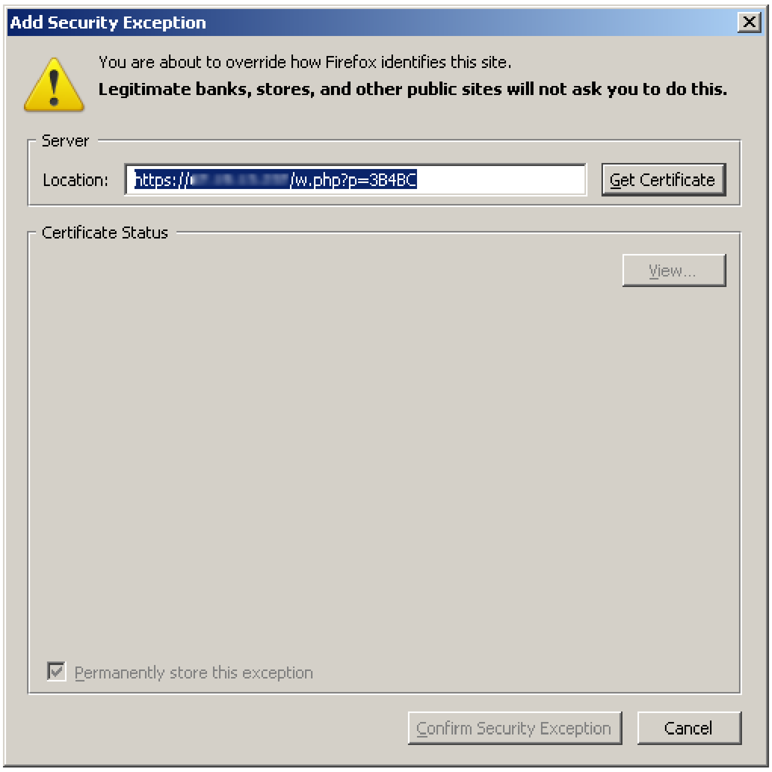
The certificate is not trusted because it is self signed.

(Error code: sec_error_ca_cert_invalid)

- This could be a problem with the server's configuration, or it could be someone trying to impersonate the server.
- If you have connected to this server successfully in the past, the error may be temporary, and you can try again later.

You should not add an exception if you are using an internet connection that you do not trust completely or if you are not used to seeing a warning for this server.

Then on "Add Exception..."



You are about to override how Firefox identifies this site.

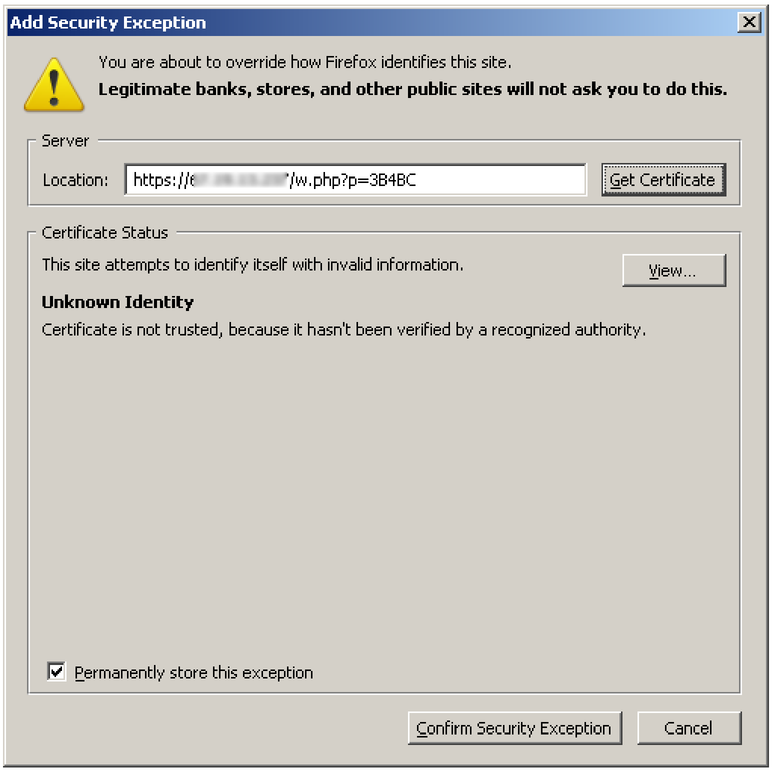
Legitimate banks, stores, and other public sites will not ask you to do this.

Server

Location: https://[redacted]/w.php?p=3B4BC

☑ Permanently store this exception

Afterwards on "Get Certificate"



Add Security Exception

You are about to override how Firefox identifies this site.

Legitimate banks, stores, and other public sites will not ask you to do this.

Server

Location: https://[redacted]/w.php?p=3B4BC

Certificate Status

This site attempts to identify itself with invalid information.

Unknown Identity

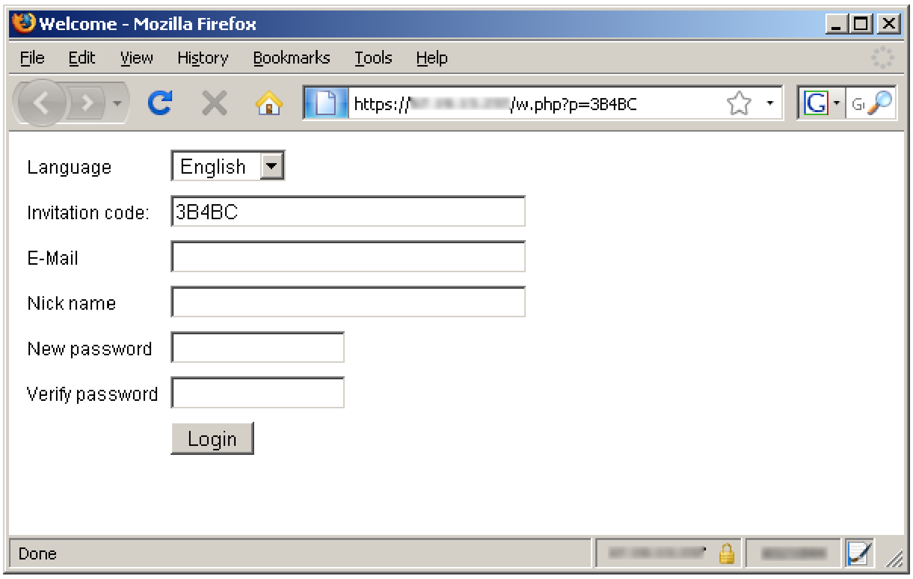
Certificate is not trusted, because it hasn't been verified by a recognized authority.

☑ Permanently store this exception

And finally "Confirm Security Exception".

Create your own account

Once you confirmed the security warning you will see a simple registration form:



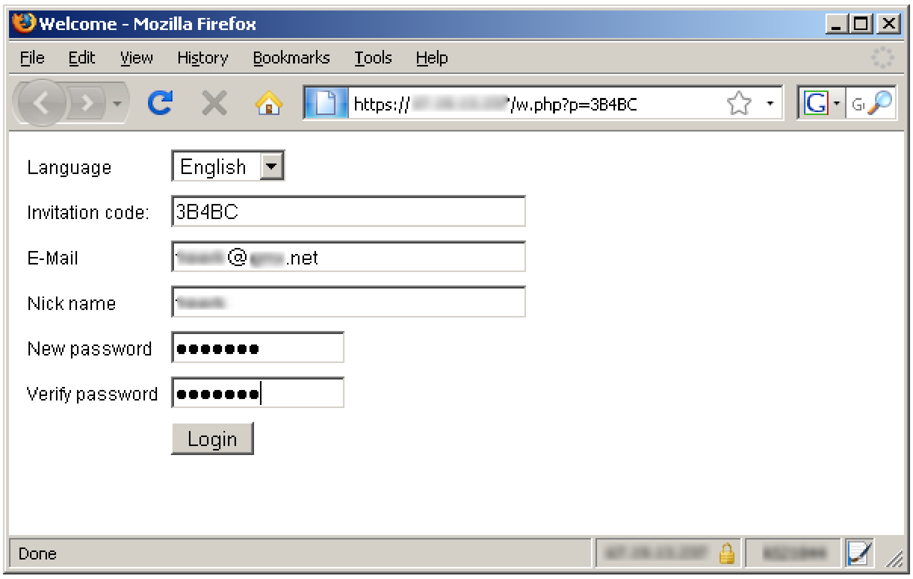
Welcome - Mozilla Firefox

https://[redacted]/w.php?p=3B4BC

Language	English
Invitation code:	3B4BC
E-Mail	
Nick name	
New password	
Verify password	

Done

Choose a language, leave the Invitation code as is and enter your email-address, a nick name and a password (two times the same). The email address will be used to send you a new psiphon2 node when this one gets blocked. We will never send spam to that address. The email-address and password you choose will be necessary to log in to the psiphon2 node later, so you have to remember them.



https://[redacted]/w.php?p=3B4BC

Language: English

Invitation code: 3B4BC

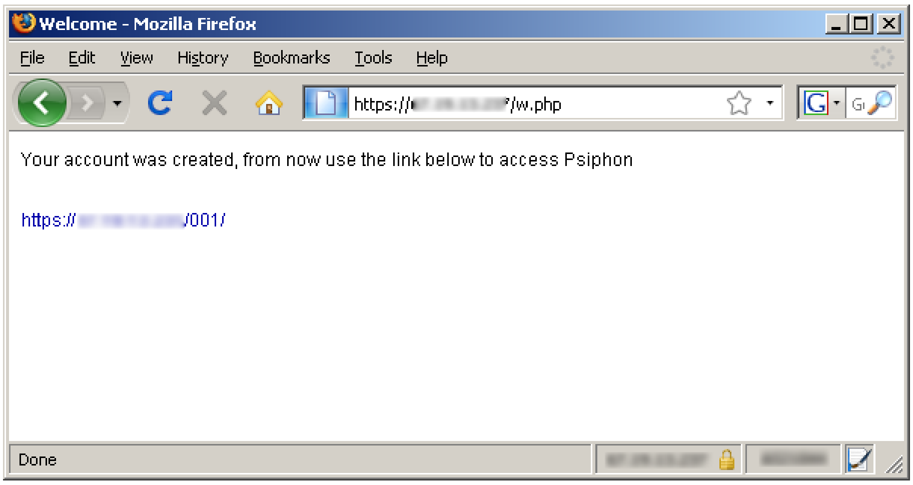
E-Mail: [redacted]@[redacted].net

Nick name: [redacted]

New password: ●●●●●●●

Verify password: ●●●●●●●●

After a click on "Login" you will see a message confirming the successful creation of your account:



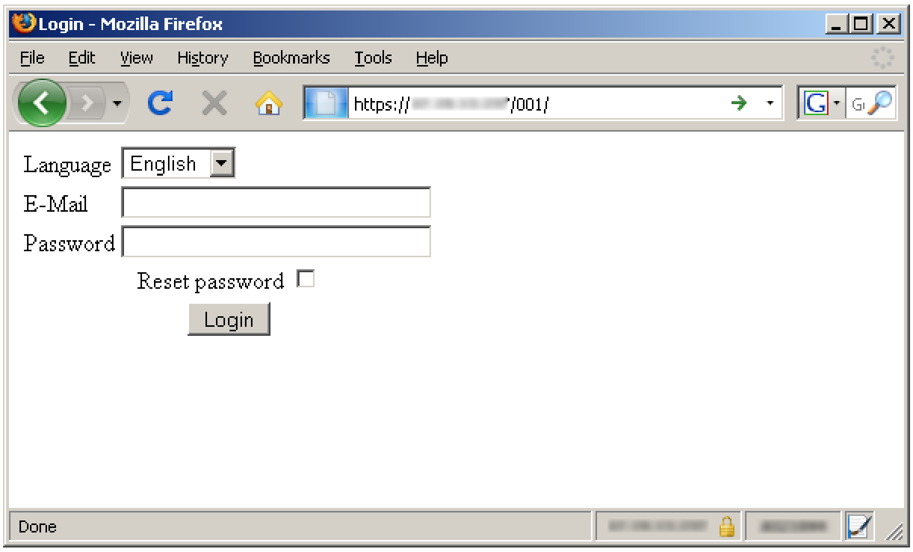
https://[redacted]/w.php

Your account was created, from now use the link below to access Psiphon

https://[redacted]/001/

Use the psiphon2 node

To use the psiphon2 node you don't need the invitation link again, just remember (for example make a bookmark) the link displayed at the end of your registration, for example "https://85.31.189.76/001/". Access that URL with your browser (for example Internet Explorer or Firefox)



https://[redacted]/001/

Language English

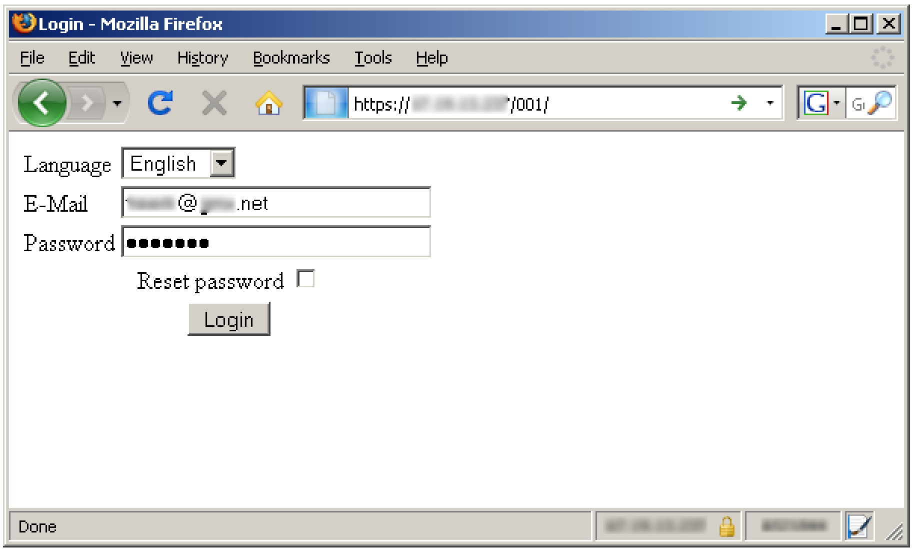
E-Mail

Password

Reset password □

Login

Now enter the email address and the password you used to register your psiphon2 account. You can also choose another language:



https://[redacted]/001/

Language English

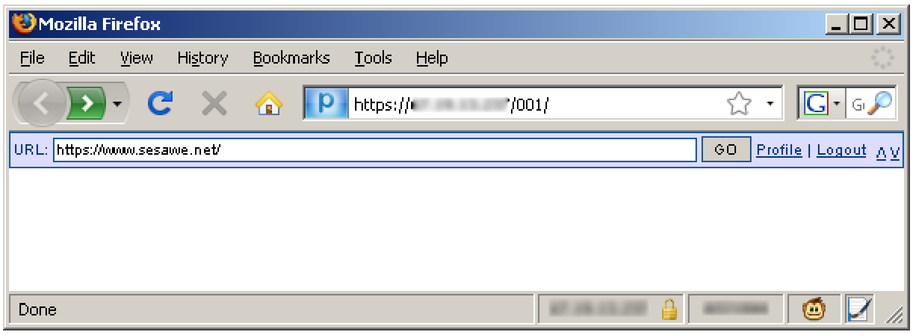
E-Mail [redacted]@[redacted].net

Password ●●●●●●●

Reset password □

Login

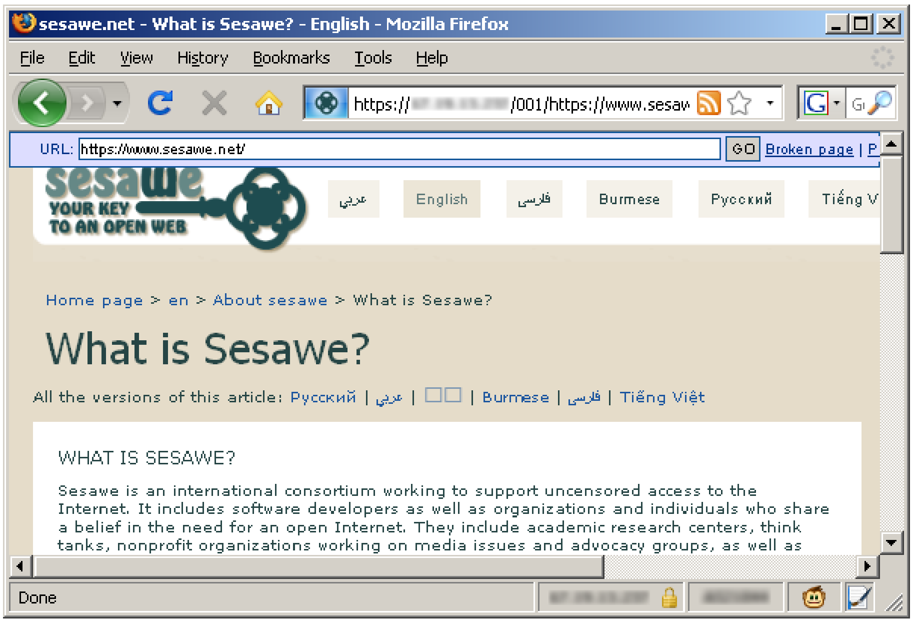
After the login you will see a white page with a small form on top. Enter the website you want to visit in that form, like "https://www.sesawe.net/" and click on "GO".



https://[redacted]/001/

URL: https://www.sesawe.net/ GO Profile | Logout

Now the website you want to visit will load and you can continue to surf the Internet freely. All the links on the website will be automatically rewritten so that they go through the psiphon2 node.



https://[redacted]/001/https://www.sesaw

URL: https://www.sesawe.net/

Home page > en > About sesawe > What is Sesawe?

What is Sesawe?

All the versions of this article: Русский | عربي | □□ | Burmese | فارسی | Tiếng Việt

WHAT IS SESAWE?

Sesawe is an international consortium working to support uncensored access to the Internet. It includes software developers as well as organizations and individuals who share a belief in the need for an open Internet. They include academic research centers, think tanks, nonprofit organizations working on media issues and advocacy groups, as well as

[redacted]

[redacted]

Invite others

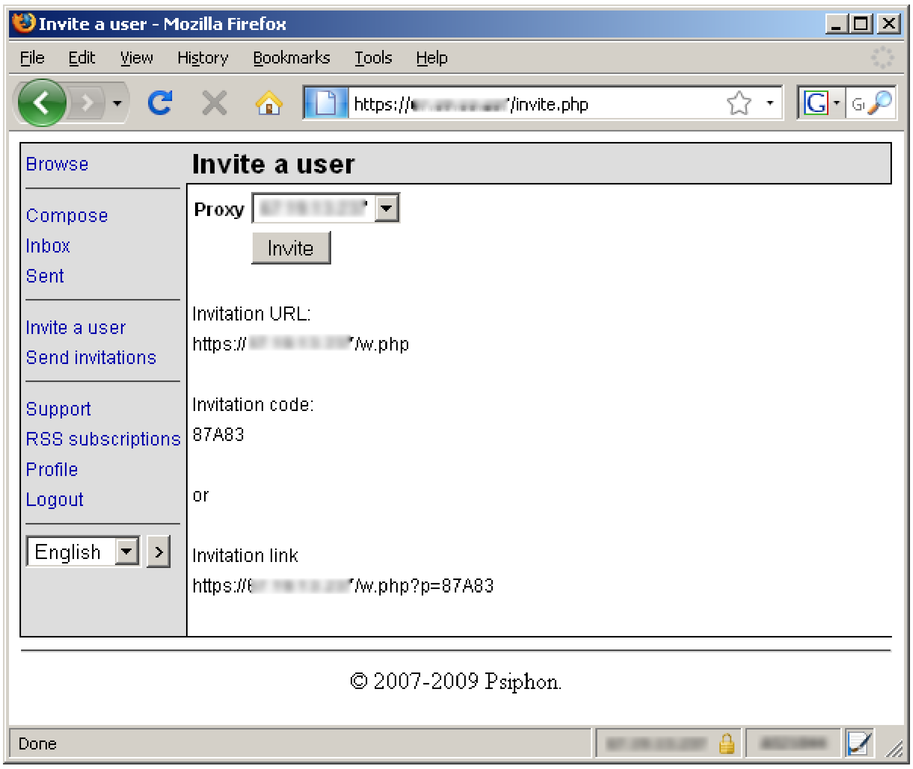
Maybe you want to help your friends or family members to access websites freely with psiphon2.

To be able to invite other people your have to be a **"Power user"**. To get that status, ask the user who invited you to grant it. You can see if you have a "Power user" account by looking in your Profile (log in to psiphon2 and click on "Profile"). If you see the links "Invite a user" and "Send invitations" in the menu on the left it means that you have "Power user" status.

There are two ways to invite other people:

Invite a user

Click on "Invite a user" in your psiphon2 profile page to generate a invitation code/link that you can communicate for example by normal email, instant messengers or telephone. First, choose the psiphon2 node for which you want so send an invitation for. It is very likely that you only have one node in the dropdown menu, so leave the default option. After a click on "Invite" you see a newly generated "Invitation link" you can send to your friends. If they have problems using it they can also try to use the "Invitation URL" and the "Invitation Code" manually.



Invite a user

Proxy [redacted]

Invitation URL:
https://[redacted]/w.php

Invitation code:
87A83

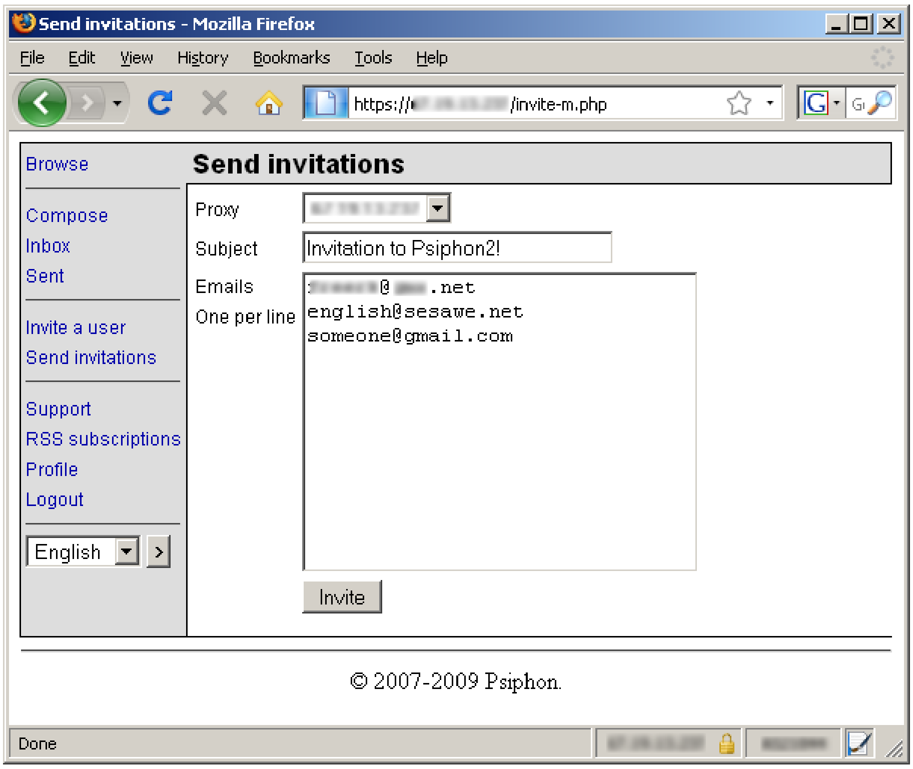
or

Invitation link
https://[redacted]/w.php?p=87A83

© 2007-2009 Psiphon.

Send invitations

Click on "Send invitations" in your psiphon2 profile to send one or more invitation links automatically through the psiphon2 node. The advantage of this method is that you stay anonymous, the receiver of the email invitation doesn't know who sent him the invitation.
First, choose the psiphon2 node for which you want so send an invitation for. It is very likely that you only have one node in the dropdown menu, so leave the default option. Then, enter a subject for the email the node will send. This can be something related like "Invitation to psiphon2" or something harmless and completely unrelated like "Praise the king!!". Then enter the email addresses which you want to receive an invitation. You can enter just one email address or many, one address per line. After a click on "Invite" you get the message "1 invitations queued" which means that the node sends out the emails in the next minutes.


Send invitations - Mozilla Firefox
File Edit View History Bookmarks Tools Help
https://[redacted]/invite-m.php
Browse
Compose
Inbox
Sent
Invite a user
Send invitations
Support
RSS subscriptions
Profile
Logout
English
Invite
Done

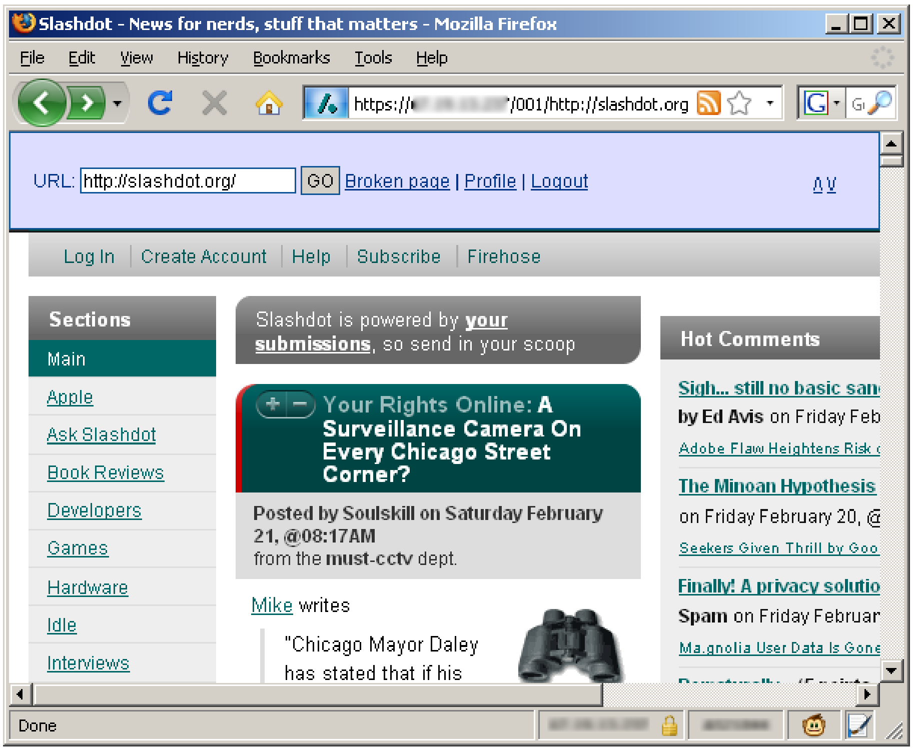
Send invitations

Proxy	[redacted]
Subject	Invitation to Psiphon2!
Emails One per line	[redacted]@[redacted].net english@sesawe.net someone@gmail.com

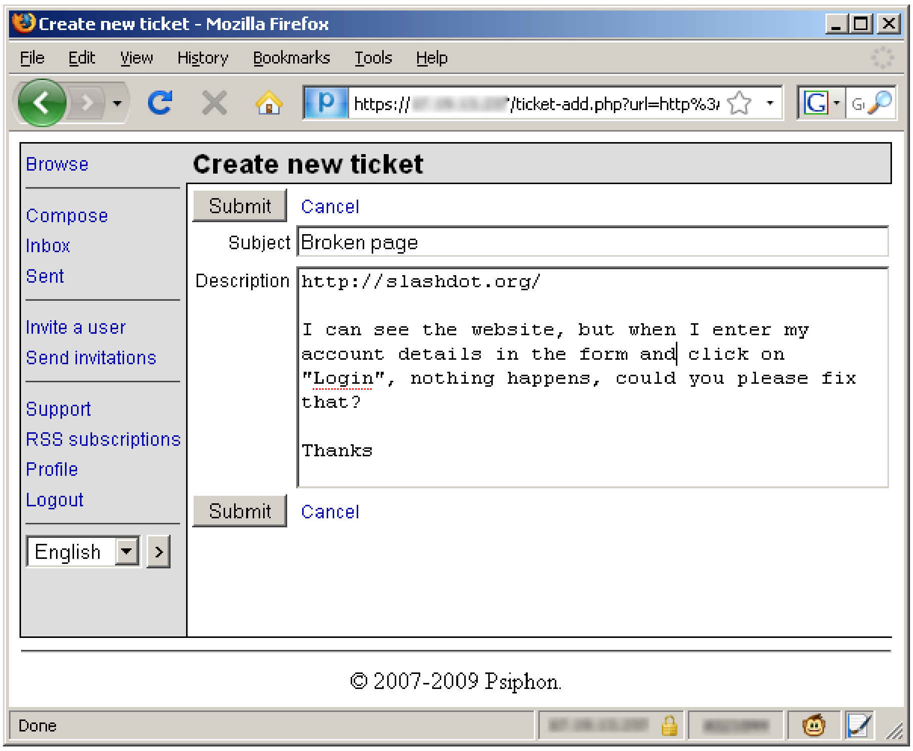
© 2007-2009 Psiphon.

Report a blocked website

Some website that use complicated technologies like streaming Video or AJAX may not work with psiphon2 out of the box. To fix it our developers have to know which websites are not working. If you find such a website you can report it easily by clicking on the "Broken Page" link close to the "GO" button of the top form:


Slashdot - News for nerds, stuff that matters - Mozilla Firefox
File Edit View History Bookmarks Tools Help
https://[redacted]/001/http://slashdot.org
URL: http://slashdot.org/
GO
Broken page | Profile | Logout
Log In | Create Account | Help | Subscribe | Firehose
Sections
Main
Apple
Ask Slashdot
Book Reviews
Developers
Games
Hardware
Idle
Interviews
Slashdot is powered by your submissions, so send in your scoop
Your Rights Online: A Surveillance Camera On Every Chicago Street Corner?
Posted by Soulskill on Saturday February 21, @08:17AM
from the must-cctv dept.
Mike writes
"Chicago Mayor Daley has stated that if his
Hot Comments
Sigh... still no basic san
by Ed Avis on Friday Feb
Adobe Flaw Heightens Risk
The Minoan Hypothesis
on Friday February 20, @
Seekers Given Thrill by Goo
Finally! A privacy solutio
Spam on Friday Februar
Ma.gnolia User Data Is Gone
Done

On the next website you can enter some additional information in the "Description" field to make it easier for the developers to reproduce the error and fix it. With a click on "Submit" you send the message to our developers.



Subject: Broken page

Description:

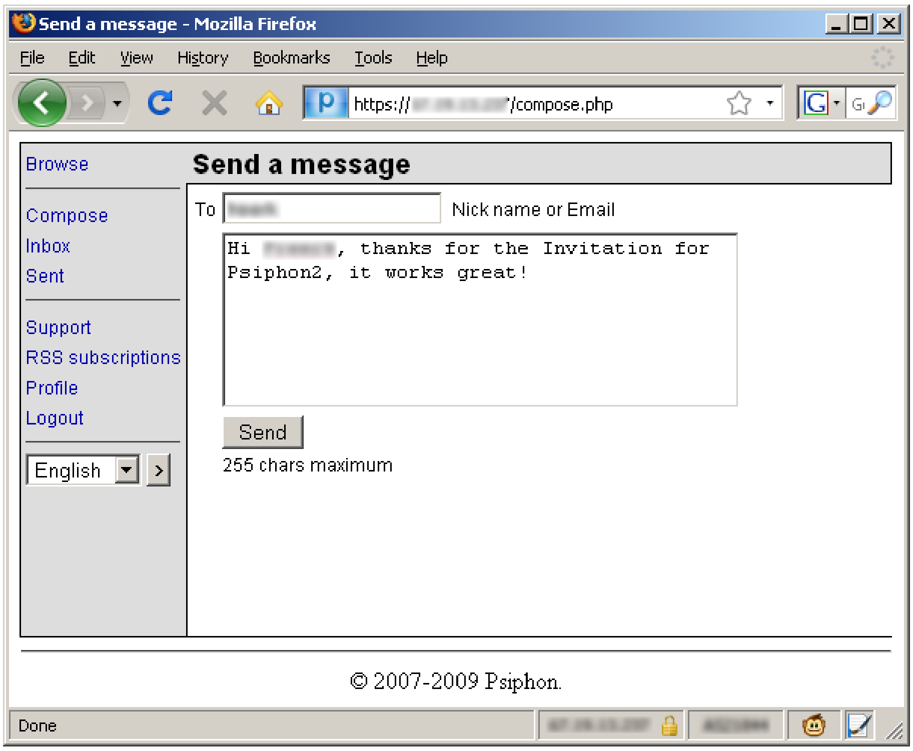
```
http://slashdot.org/

I can see the website, but when I enter my
account details in the form and click on
"Login", nothing happens, could you please fix
that?

Thanks
```

© 2007-2009 Psiphon.

Use Psimail

Send messages

With psiphon2 it is possible to send internal messages to other psiphon2 users. To write a message enter in your psiphon2 profile and click on "Compose". In the first form enter the nickname of the user you want to send a message to. You can also enter the email address the other user used to register as psiphon2. Please note that it is not possible to send messages to normal email addresses which are not registered at psiphon2. Write your message in the textbox and click on "Send". You will then get the message "Message was sent".


Send a message - Mozilla Firefox
File Edit View History Bookmarks Tools Help
Browse
Compose
Inbox
Sent
Support
RSS subscriptions
Profile
Logout
English
Send
Done

Send a message

https://[redacted]/compose.php

To [redacted] Nick name or Email

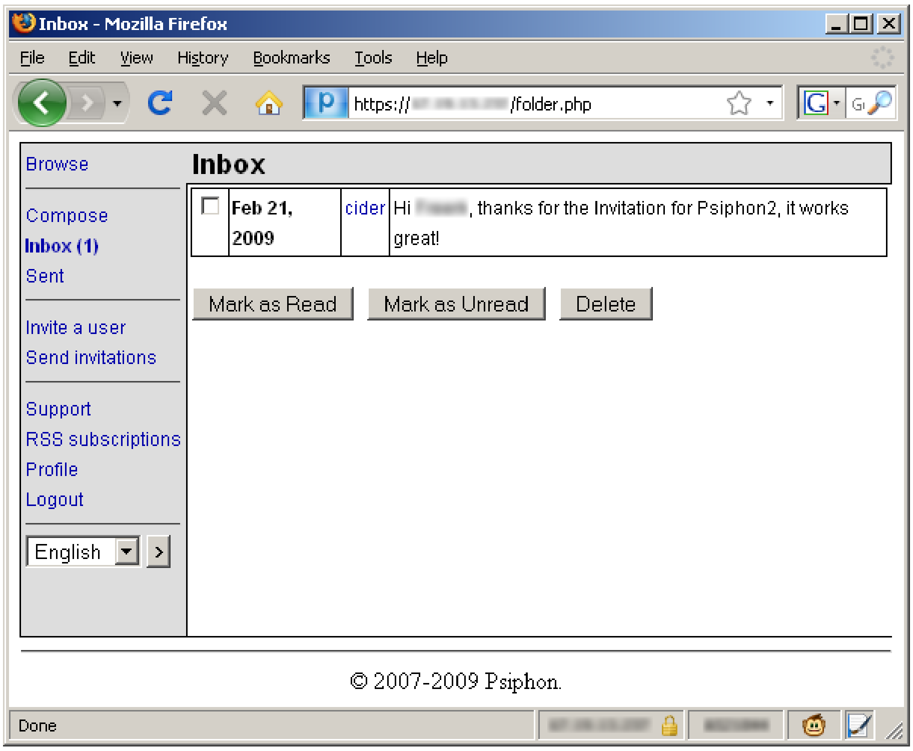
```
Hi [redacted], thanks for the Invitation for
Psiphon2, it works great!
```

255 chars maximum

© 2007-2009 Psiphon.

Read Messages

To see if you received a new messages enter your psiphon2 profile. If you see a bold "Inbox (1)" in the menu on the left, you have new messages. The number in brackets stands for the number of new messages. After a click on the link you can read the messages:



Inbox

https://[redacted]/folder.php

□	**Feb 21, 2009**	cider	Hi [redacted], thanks for the Invitation for Psiphon2, it works great!

© 2007-2009 Psiphon.

You can check one or more messages and select one of the possible options: "Mark as Read", "Mark as Unread" or "Delete".

More resources

Psiphon2 FAQ at sesawe.net: https://www.sesawe.net/Psiphon-FAQ.html

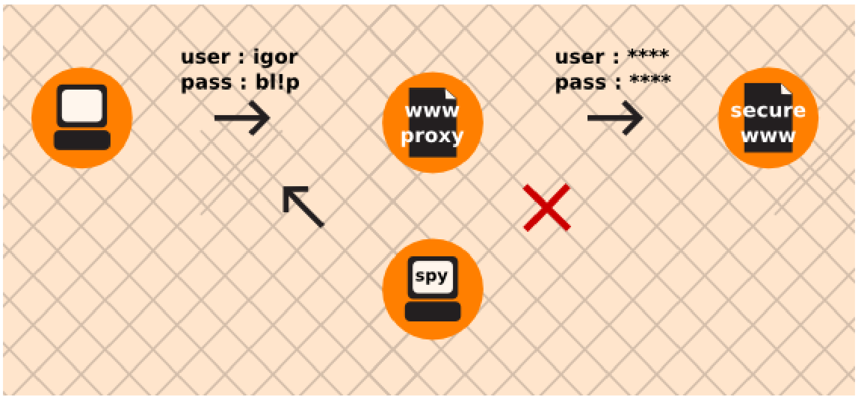
Web Proxy Risks

You should be aware of some of the risks associated with the use of **Web proxies**, especially those maintained by people or organizations you do not know. If you use a proxy to view a public Web site like npr.org, your only risk is that someone will know you were reading the news there (and using a proxy to do it). However, if you use a proxy to send private communications or to reach applications like Web mail, online banking or shopping, there is a risk that other people could access and misuse your information, including your private passwords, especially if those services don't use encryption or if the proxy prevents you from using that encryption.

Lack of Privacy

Systems to circumvent filtering or blocking do not necessarily provide anonymity (even those that may include words like "anonymizer" in their names!). If the link between you and the Web proxy is unencrypted (**HTTP** as opposed to **HTTPS**), as with many free Web proxy services, either the operator of the proxy or an intermediary such as an **Internet Service Provider** (ISP) can intercept and analyze the content. In that case, although circumvention may be successful, network operators can still track the fact that you have used a Web proxy and can determine the content and Web sites you visited.

A Web proxy that does not encrypt your connection sometimes uses other methods to avoid Internet filtering. For example, one simple technique is called ROT-13, in which the current letter of a URL is replaced by the one that is thirteen characters ahead of it in the standard Latin alphabet. (You can try it yourself at http://www.rot13.com/) Using ROT-13, the URL http://ice.citizenlab.org becomes uggc://vpr.pvgvmrayno.bet -- making it unrecognizable to a keyword filter. This may help you in reaching your Web destination, but has its weaknesses: the content of the session can still be detected and such measures can easily be reversed.

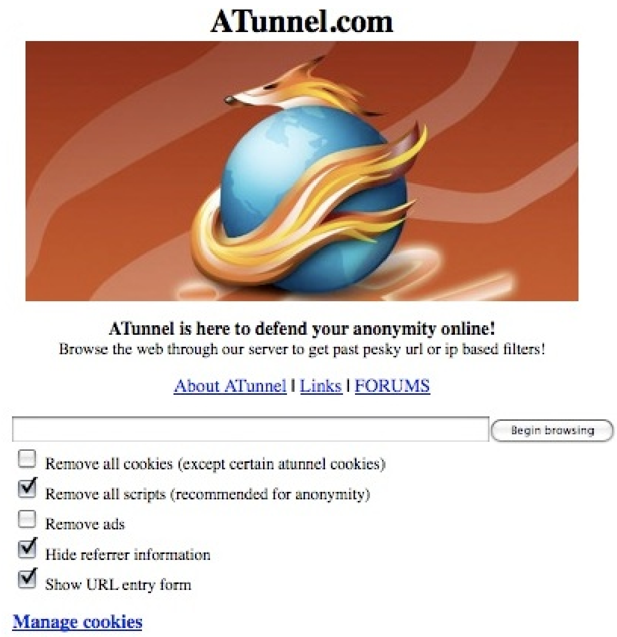


Advertising, viruses and malware

Some of the people who set up Web proxies do it to make money. This may be done simply and openly by selling advertisements on the pages. More maliciously, some proxy operators may try to infect the computers of those using their proxies with **malware**, or malicious software. These so-called "drive-by-downloads" can hijack your computer for spamming or other commercial or even illegal purposes.

The most important things you can do to protect against viruses is to keep all of your software -- including your operating system -- updated and to use an up-to-date antivirus scanner. You can also block ads by using the AdBlockPlus Extension for the Firefox Browser (http://www.adblockplus.org/). More information on avoiding these risks can be found at the StopBadware Web site (http://www.stopbadware.org/).

The operator of ATunnel.com supports the free service by selling advertisements (in this example for razors). This is a typical example of an ad-supported proxy server.



ATunnel.com

ATunnel is here to defend your anonymity online!
Browse the web through our server to get past pesky url or ip based filters!

About ATunnel | Links | FORUMS

☐ Remove all cookies (except certain atunnel cookies)
☑ Remove all scripts (recommended for anonymity)
☐ Remove ads
☑ Hide referrer information
☑ Show URL entry form

Manage cookies

Cookies and scripts

There are also risks concerning the use of **cookies** and scripts. Many Web proxies can be configured to remove cookies and scripts, but many sites (for example, social networking sites like MySpace) require the use of cookies and scripts. Be careful when enabling these options, because the cookies may be saved on your computer even after you restart it, and so could provide evidence of which sites you visited. One option is to allow selective use of Cookies. In Firefox 3, for instance, you can instruct the browser to accept cookies only "Until I close Firefox". (Similarly, you can instruct your browser to erase your browsing history when you close it.)

Some sites and advertisers can use these mechanisms to track you even when you use proxies. If you are trying to be anonymous, this can be a problem because this tracking can produce evidence, for example, that the person who did one thing openly is the same person who did another thing anonymously.

The proxy operator can see everything

Even though your connection to the Web-based circumventor may be secure (encrypted), the owner of the proxy will have access to the content of your communications after decrypting them. An additional security concern is the records (log files) that the proxy provider may keep. Depending on the circumventor's location, or the location of their server, authorities may have access to those log files.

Advanced Background

There can be many reasons why simple techniques for accessing blocked content, such as using cached versions of pages from a search engine, or using a simple Web proxy, are inadequate.

In some cases, these simple techniques aren't enough to get around the blocking. In others, the restrictions may affect services beyond simple Web browsing -- such as instant messaging, e-mail or video streaming. In that case, Web proxies probably won't solve your problem.

There may be cases when you want to bypass Internet blocking, but also want to prevent the organization doing the blocking from knowing what pages you are accessing, or prevent them from knowing you are even bypassing filters in the first place.

In these scenarios, there are many more advanced techniques available, and each of them solves different problems in different ways.

This chapter introduces some key technical concepts that will help you make an informed choice about which solution is applicable in a given situation. It also covers, in some detail, many of the different ways access to information may be blocked.

Ports and Protocols

The Internet is based on a series of **protocols**, standardized sets of rules that govern how the networks of computers communicate. The principal set of protocols for managing connections and message packets for the Internet is TCP/IP (TCP over IP). Protocols can handle a wide range of data, with software to break long transmissions into smaller, numbered packets for transmission, and reassemble the data segments on the receiving end. The most common way to specify which protocol to use is to address packets to a specific port number. For example, HTTP for the Web normally uses port 80, and POP3 for receiving e-mail normally uses port 110. Blocking traffic to a particular port at a particular IP address disables normal access to one service at that site, while leaving the rest of the services available. The simplest way to circumvent a blocked port is to provide the service on a non-standard port, but this can only be done by the operator of the service, not by the user.

The layered networking model

Network protocols are often described as existing in a set of layers. For the Internet, the bottom layer (called the **Link Layer**) is closest to the hardware, and the highest (called the **Application Layer**) is closest to the human user. The critical protocols in the middle two layers are **TCP (Transmission Control Protocol)**, which is in the **Transport Layer**, and **IP (Internet Protocol)**, which is "below" it in the **Internet Layer**. The two together are commonly referred to as TCP/IP. Less well known but also important is **UDP (User Datagram Protocol)**, which is at the same level as TCP. Many, but not all services offered over TCP are also available over UDP, while some services are on UDP only.

The top level, called the **Application Layer**, includes protocols such as **DNS** (for domain names), **FTP** (file transfers), **HTTP** (Web), **IRC** (chat), **NNTP** (Usenet), **POP3** (retrieving e-mail), **SIP** (Voice-over-IP), and **SSH** (encrypted communications). IANA (Internet Assigned Names Authority) assigns port numbers for each of these application services, such as port 53 for DNS lookup queries, 80 for HTTP, and 110 for POP3 (Post Office Protocol 3). These assignments are *defaults*, for convenience, and using them is not generally a technical requirement of the protocols; in fact, any sort of data could be sent over any port. There are also numerous default port assignments for UDP that operate in the same way. In some, but by no means all, cases, a service can be accessed on the same port using either TCP or UDP. One exception is NTP (Network Time Protocol), which is one that is provided only on UDP. UDP is also commonly used for real-time multimedia applications such as Voice over IP (VoIP) protocols, some of which are not available over TCP.

Users are normally not concerned with port assignments, which are handled automatically in the default cases. Use of the standard ports is not mandatory, however. By prior arrangement between service providers and users, system administrators can set up servers for access to standard services at non-standard port numbers. This allows software to circumvent simple port blocks intended to prevent use of these services.

Some software can be configured to use a non-standard port number. URLs also have a particularly convenient standard way of specifying a port number inside the URL. For example, the URL `http://www.example.com:8000/foo/`would make an HTTP request to example.com on port 8000, rather than the default http port 80.

Advanced Filtering Techniques

[Adapted from "Access Denied", Chapter 3, by Steven J. Murdoch and Ross Anderson]

The goals of deploying a filtering mechanism vary depending on the motivations of the organization deploying them. They may be to make a particular Web site (or individual Web page) inaccessible to those who wish to view it, to make it unreliable, or to deter users from even attempting to access it in the first place. The choice of mechanism will also depend upon the capability of the organization that requests the filteringâ where they have access to, the people against whom they can enforce their wishes, and how much they are willing to spend. Other considerations include the number of acceptable errors, whether the filtering should be overt or covert, and how reliable it is (both against casual users and those who wish to bypass it).

In this section we will describe how particular content can be blocked once the list of resources to be blocked is established. Building this list is a considerable challenge and a common weakness in deployed systems. Not only does the huge number of Web sites make building a comprehensive list of prohibited content difficult, but as content moves and Web sites change their IP addresses, keeping this list up-to-date requires a lot of effort. Moreover, if the operator of a site wishes to interfere with the blocking, the site could be moved more rapidly than it would be otherwise.

TCP/IP Header Filtering

An IP packet consists of a header followed by the data the packet carries (the payload). Routers must inspect the packet header, as this is where the destination IP address is located. To prevent targeted hosts being accessed, routers can be configured to drop packets destined for IP addresses on a blacklist. However, each host may provide multiple services, such as hosting both Web sites and e-mail servers. Blocking based solely on IP addresses will make all services on each blacklisted host inaccessible.

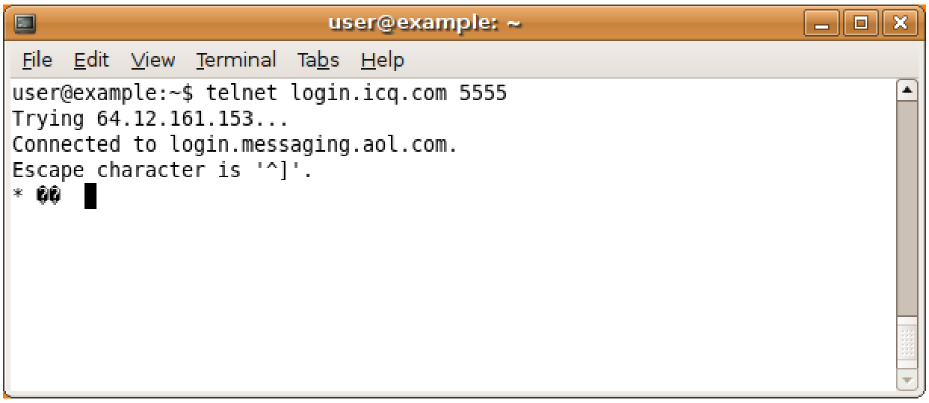
Slightly more precise blocking can be achieved by additionally blacklisting the port number, which is also in the TCP/IP header. It is very common for many completely different web-sites to be hosted on the same IP-number, on the same port number, 80.

Port Blocking

Access to ports may be controlled by the network administrator of the organization that hosts the computer you're using -- whether a private company or an Internet cafÃ©, by the ISP that is providing Internet access, or by someone else such as a government censor who has access to the connections that are available to the ISP. There are many reasons other than censorship that ports may be blocked -- to reduce spam, or to control costs associated with high-bandwidth uses such as peer-to-peer filesharing.

If a port is blocked, all traffic on this port becomes inaccessible to you. Censors often block the ports 1080, 3128, and 8080 because these are the most common proxy ports. If this is the case, you have to find proxies that are listening on an uncommon port. These can be difficult to find.

You can test which ports are blocked on your connection using Telnet. Just open a command line (terminal or DOS prompt), type "telnet login.icq.com 5555" or "telnet login.oscar.aol.com 5555" and press Enter. The number is the port you want to test. If you get some strange symbols in return, the connection succeeded.



```
user@example:~$ telnet login.icq.com 5555
Trying 64.12.161.153...
Connected to login.messaging.aol.com.
Escape character is '^]'.
* ��
```

If, on the other hand, the computer immediately reports that the connection failed, timed out, or was interrupted, disconnected, or reset, that port is probably being blocked. (Keep in mind that some ports could be blocked only in conjunction with certain IP addresses.)

Some of the most commonly used ports are:

- 20 and 21 - FTP (file transfer)
- 22 - SSH (secure shell remote access)
- 23 - Telnet (unsecure remote access)
- 25 - SMTP (send email)
- 53 - DNS (resolves a computer's name to an IP address)
- 80 - HTTP (normal web browsing; also sometimes used for a proxy)
- 110 - POP3 (receive email)
- 143 - IMAP (send/receive email)
- 443 - SSL (secure HTTPS connections)
- 993 - secure IMAP
- 995 - secure POP3
- 1080 - SOCKS proxy
- 1194 - OpenVPN
- 3128 - Squid proxy
- 3389 - Remote Desktop
- 8080 - Standard HTTP-style proxy

For example, in one university, only the ports 22 (SSH), 110 (POP3), 143 (IMAP), 993 (secure IMAP), 995 (secure POP3) and 5190 (ICQ instant messaging) may be open for external connections. This means that you would need to find a proxy server or VPN server running on one of these ports, or convince a friend or contact outside the university to set up a server on such a port. The ability to run servers on ports others than those they normally run on is what makes several circumvention techniques possible in the first place.

TCP/IP Content Filtering

TCP/IP header filtering can only block communication on the basis of where packets are going to or coming from, not what they contain. This can be a problem for the censor if it is impossible to establish the full list of IP addresses containing prohibited content, or if some IP address contains enough non-infringing content to make it seem unjustifiable to totally block all communication with it. There is a finer-grained control possible:

the content of packets can be inspected for banned keywords. As routers do not normally examine packet content but just packet headers, extra equipment may be needed. Typical hardware may be unable to react fast enough to block the infringing packets, so other means to block the information must be used instead. As packets have a maximum size, the full content of the communication will likely be split over multiple packets. Thus while the offending packet will get through, the communication can be disrupted by blocking subsequent packets. This may be achieved by blocking the packets directly or by sending a message to both of the communicating parties requesting they terminate the conversation. Another effect of the maximum packet size is that keywords may be split over packet boundaries. Devices that inspect each packet individually may then fail to identify infringing keywords. For packet inspection to be fully effective, the stream must be reassembled, which adds additional complexity. Alternatively, an HTTP proxy filter can be used, as described later.

DNS Tampering

Most Internet communication uses domain names rather than IP addresses, particularly for Web browsing. Thus, if the domain name resolution stage can be filtered, access to infringing sites can be effectively blocked. With this strategy, the DNS server accessed by users is given a list of banned domain names. When a computer requests the corresponding IP address for one of these domain names, an erroneous (or no) answer is given. Without the IP address, the requesting computer cannot continue and will display an error message.

Note that at the stage the blocking is performed, the user has not yet requested a page, which is why all pages under a domain name will be blocked.

HTTP Proxy Filtering

An alternative way of configuring a network is to not allow users to connect directly to Web sites but force (or just encourage) all users to access those sites via a proxy server. In addition to relaying requests, the proxy server may temporarily store the Web page in a cache. The advantage of this approach is that if a second user of the same ISP requests the same page, it will be returned directly from the cache, rather than connecting to the actual Web server a second time. From the userâ s perspective this is better since the Web page will appear faster, as they never have to connect outside their own ISP. It is also better for the ISP, as connecting to the Web server will consume (expensive) bandwidth, and rather than having to transfer pages from a popular site hundreds of times, they need only do this once.

However, as well as improving performance, an HTTP proxy can also block Web sites. The proxy decides whether requests for Web pages should be permitted, and if so, sends the request to the Web server hosting the requested content. Since the full content of the request is available, individual Web pages can be filtered, based on both page names and the actual content of the page.

Hybrid TCP/IP and HTTP Proxy

As the requests intercepted by an HTTP proxy must be reassembled from the original packets, decoded, and then retransmitted, the hardware required to keep up with a fast Internet connection is very expensive. So systems exist that provide the versatility of HTTP proxy filtering at a lower cost. They operate by building a list of the IP addresses of sites hosting prohibited content, but rather than blocking data flowing to these servers, the traffic is redirected to a transparent HTTP proxy. There, the full Web address is inspected and if it refers to banned content, it is blocked; otherwise the request is passed on as normal.

Denial of Service

Where the organization deploying the filtering does not have the authority (or access to the network infrastructure) to add conventional blocking mechanisms, Web sites can be made inaccessible by overloading the server or network connection. This technique, known as a Denial-of-Service (DoS) attack, could be mounted by one computer with a very fast network connection; more commonly, a large number of computers are taken over and used to mount a distributed DoS (DDoS).

Domain Deregistration

As mentioned earlier, the first stage of a Web request is to contact the local DNS server to find the IP address of the desired location. Storing all domain names in existence would be infeasible, so instead so-called recursive resolvers store pointers to other DNS servers that are more likely to know the answer. These servers will direct the recursive resolver to further DNS servers until one, the "authoritative" server, can return the answer.

The domain name system is organized hierarchically, with country domains such as ".uk" and ".de" at the top, along with the nongeographic top-level domains such as ".org" and ".com". The servers responsible for these domains delegate responsibility for subdomains, such as example.com, to other DNS servers, directing requests for these domains there. Thus, if the DNS server for a top-level domain deregisters a domain name, recursive resolvers will be unable to discover the IP address and so make the site inaccessible.

Country-specific top-level domains are usually operated by the government of the country in question, or by an organization appointed by it. So if a site is registered under the domain of a country that prohibits the hosted content, it runs the risk of being deregistered.

Server Takedown

Servers hosting content must be physically located somewhere, as must the administrators who operate them. If these locations are under the legal or extra-legal control of someone who objects to the content hosted, the server can be disconnected or the operators can be required to disable it.

Surveillance

The above mechanisms inhibit the access to banned material, but are both crude and possible to circumvent. Another approach, which may be applied in parallel to filtering, is to monitor which Web sites are being visited. If prohibited content is accessed (or attempted to be accessed) then legal (or extra-legal) measures could be deployed as punishment.

If this fact is widely publicized, it could discourage others from attempting to access banned content, even if the technical measures for preventing access are inadequate by themselves.

Cryptography

Cryptography is -- among other applications -- a technical defense against surveillance that uses sophisticated mathematical techniques to scramble communications, making them unintelligible to an eavesdropper. Cryptography can also prevent a network operator from modifying communications, or at least make such modifications detectable.

Modern cryptography is thought to be extremely difficult to defeat by technical means; widely available cryptographic software can give users very powerful privacy protection against eavesdropping. On the other hand, encryption can be circumvented by several means, including targeted **malware**, or in general through **key-management** and **key-exchange** problems, when users cannot or do not follow the procedures necessary to use cryptography securely. For example, cryptographic applications usually need a way to verify the identity of the person or computer at the other end of a network connection; otherwise, the communication could be vulnerable to a **man-in-the-middle attack** where an eavesdropper impersonates one's communication partner in order to intercept supposedly private communications. This identity verification is handled in different ways by different software, but skipping or bypassing the verification step can increase one's vulnerability to surveillance.

Another surveillance technique is **traffic analysis**, where facts *about* a communication are used to infer something about the content, origin, destination, or meaning of the communication even if an eavesdropper is unable to understand the *contents* of the communication. Traffic analysis can be a very powerful technique and is very difficult to defend against; it is of particular concern for anonymity systems, where traffic analysis techniques might help identify an anonymous party. Advanced anonymity systems like Tor contain some measures intended to reduce the effectiveness of traffic analysis, but might still be vulnerable to it depending on the capabilities of the eavesdropper.

Social Techniques

Social mechanisms are often used to discourage users from accessing inappropriate content. For example, families may place the PC in the living room where the screen is visible to all present, rather than somewhere more private, as a low-key way of discouraging children from accessing unsuitable sites. A library may well situate PCs so that their screens are all visible from the librarianâ s desk. An Internet cafÃ© may have a CCTV surveillance camera. There might be a local law requiring such cameras, and also requiring that users register with government-issue photo ID. There is a spectrum of available control, ranging from what many would find sensible to what many would find objectionable.

What Is A HTTP Proxy?

Software called an **application proxy** enables one computer on the Internet to process requests from another computer. The most common kinds of application proxies are **HTTP proxies**, which handle requests for Web sites, and **SOCKS proxies**, which handle connection requests from a wide variety of applications. In this chapter we will look at HTTP proxies and how they work.

Good proxies and bad proxies

Application proxies can be used by **network operators** to censor the Internet or to monitor and control what users do. However, application proxies are also a tool for users to get around censorship and other network restrictions.

Proxies that restrict access

A network operator may *require* users to access the Internet (or at least Web pages) only through a certain proxy. The network operator can program this proxy to keep records of what users access and also deny access to certain sites or services (IP blocking or port blocking). In this case, the network operator may use a **firewall** to block connections that do not go through the restrictive proxy. This configuration is sometimes called a **forced proxy**, because users are required to use it.

Proxies for circumvention

However, an application proxy can also be helpful for circumventing restrictions. If you can communicate with a computer in an unrestricted location that is running an application proxy, you can benefit from its unrestricted connectivity. Sometimes a proxy is available for the public to use; in that case, it's called an **open proxy**. Many open proxies are blocked in Internet-restricting countries if the people administering the network restrictions know about them.

Where to find an application proxy

There are many Web sites with lists of open application proxies. An overview of such Web sites is available at http://www.dmoz.org/Computers/Internet/Proxying_and_Filtering/Hosted_Proxy_Services/Free/Proxy_Lists/.

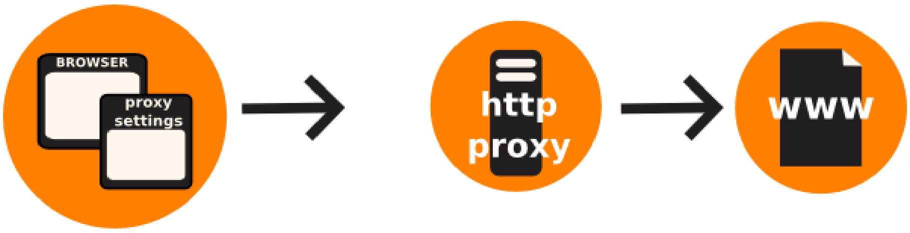
Please note that many open application proxies only exist for a few hours, so it is important to get a proxy from a list which was very recently updated.

HTTP Proxy settings

To use an application proxy, you must configure the proxy settings for your operating system or within individual applications. Once you have selected a proxy in an application's proxy settings, the application tries to use that proxy for all of its Internet access. Be sure you make note of the original settings so that you can restore them. If the proxy becomes unavailable or unreachable for some reason, the software that is set to use it generally stops working. In that case, you may need to reset to the original settings.

On Mac OS X and some Linux systems, these settings can be configured in the operating system, and will automatically be applied to applications such as the web browser or instant messaging applications. On Windows and some Linux systems, there is no central place to configure proxy settings, and each application must be configured locally. Bear in mind, that even if the proxy settings are configured centrally there is no guarantee that applications will support these settings, so it is always a good idea to check the settings of each individual application.

Typically only Web browsers can directly use an HTTP proxy.



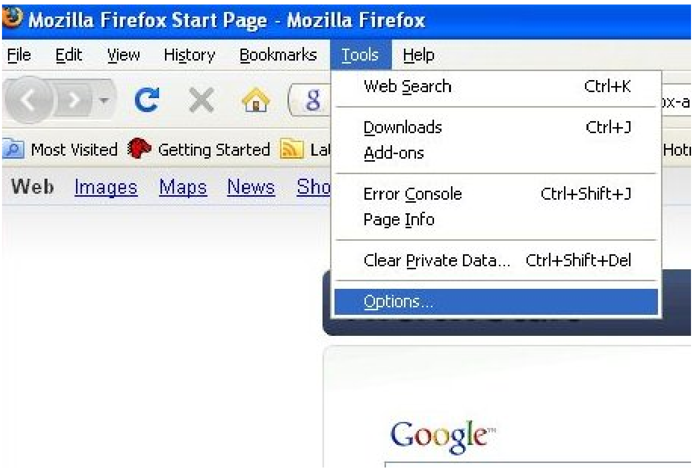
The steps below describe how to configure either Microsoft Internet Explorer, Mozilla Firefox and the Free and Open Source Instant Messaging Client Pidgin to use a proxy. If you use Firefox for Web browsing, it may be simpler to use the SwitchProxy software; it is an alternative to the steps below. If you use Tor, it is safest to use the TorButton software (which is provided as part of the Tor Bundle download) to configure your browser to use Tor.

While e-mail clients such as Microsoft Outlook and Mozilla Thunderbird can also be configured to use HTTP proxies, actual mail traffic when sending and fetching mail, uses other protocols such as POP3, IMAP and SMTP, and this traffic will not pass through the HTTP proxy.

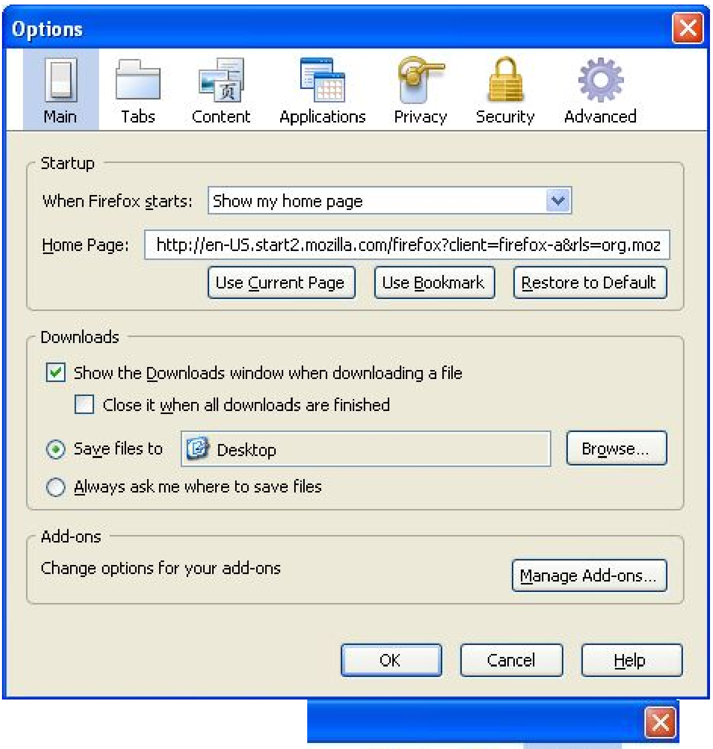
Mozilla Firefox

To configure Firefox to use an HTTP proxy:

1. On the "Tools" menu, click "Options":



2.



Startup

When Firefox starts: Show my home page

Home Page: http://en-US.start2.mozilla.com/firefox?client=firefox-a&rls=org.moz

Downloads

☑ Show the Downloads window when downloading a file

□ Close it when all downloads are finished

● Save files to Desktop

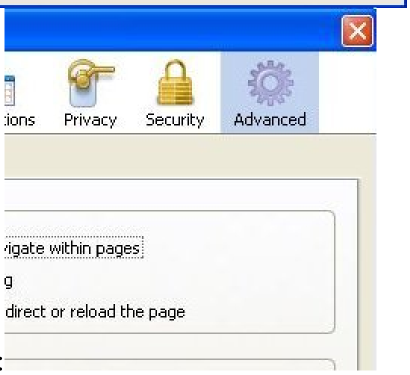
○ Always ask me where to save files

Add-ons

Change options for your add-ons

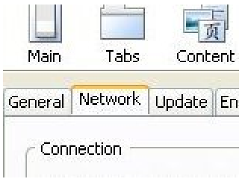
The "Options" window appears:

3.



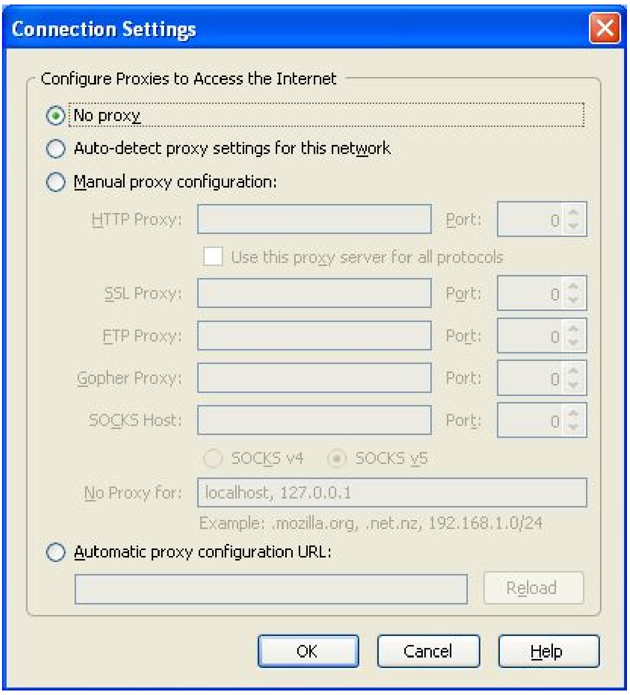
In the toolbar at the top of the window, click "Advanced":

4. Click the "Network" tab:



5. Click "Settings". Firefox displays the "Connection Settings"

window:



Connection Settings

Configure Proxies to Access the Internet

● No proxy

○ Auto-detect proxy settings for this network

○ Manual proxy configuration:

HTTP Proxy: Port: 0

□ Use this proxy server for all protocols

SSL Proxy: Port: 0

FTP Proxy: Port: 0

Gopher Proxy: Port: 0

SOCKS Host: Port: 0

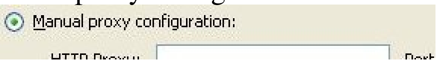
○ SOCKS v4 ● SOCKS v5

No Proxy for: localhost, 127.0.0.1

Example: .mozilla.org, .net.nz, 192.168.1.0/24

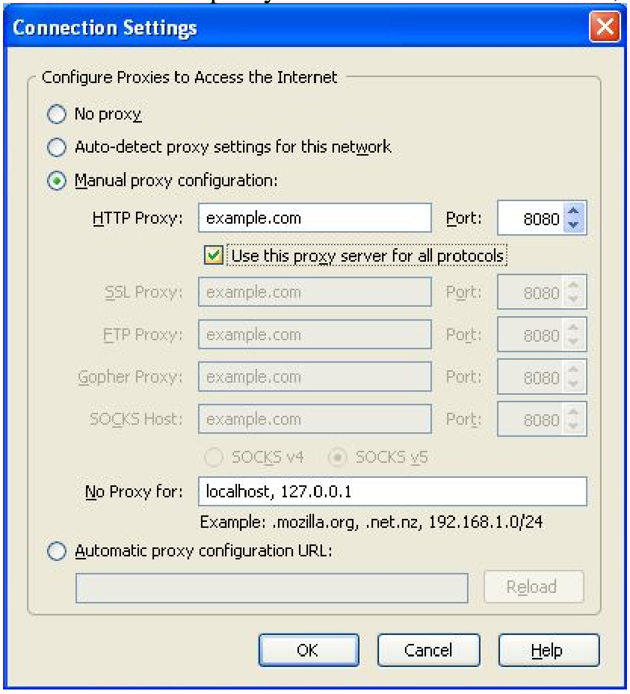
○ Automatic proxy configuration URL:

6. Select "Manual proxy configuration". The fields below that option become available.



● Manual proxy configuration:

7. Enter the "HTTP proxy" address and "Port" number, and then click "OK".



Connection Settings

Configure Proxies to Access the Internet

○ No proxy

○ Auto-detect proxy settings for this network

● Manual proxy configuration:

HTTP Proxy: example.com Port: 8080

☑ Use this proxy server for all protocols

SSL Proxy: example.com Port: 8080

FTP Proxy: example.com Port: 8080

Gopher Proxy: example.com Port: 8080

SOCKS Host: example.com Port: 8080

○ SOCKS v4 ● SOCKS v5

No Proxy for: localhost, 127.0.0.1

Example: .mozilla.org, .net.nz, 192.168.1.0/24

○ Automatic proxy configuration URL:

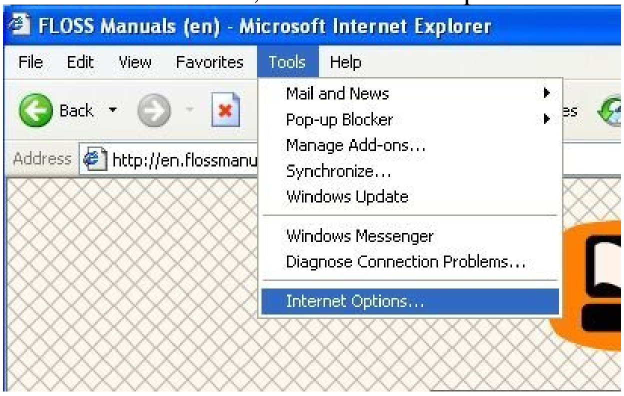
If you click the "Use this proxy server for all protocols", Firefox will attempt to send HTTPS (secure HTTP) and FTP traffic through the proxy. This may not work if you are using a public application proxy, since many of these do not support HTTPS and FTP traffic. If, on the other hand your HTTPS and/or FTP traffic is being blocked, you can try to find a public application proxy with HTTPS and/or FTP support, and use the "Use this proxy server for all protocols" setting in Firefox.

Now Firefox is configured to use an HTTP proxy.

Microsoft Internet Explorer

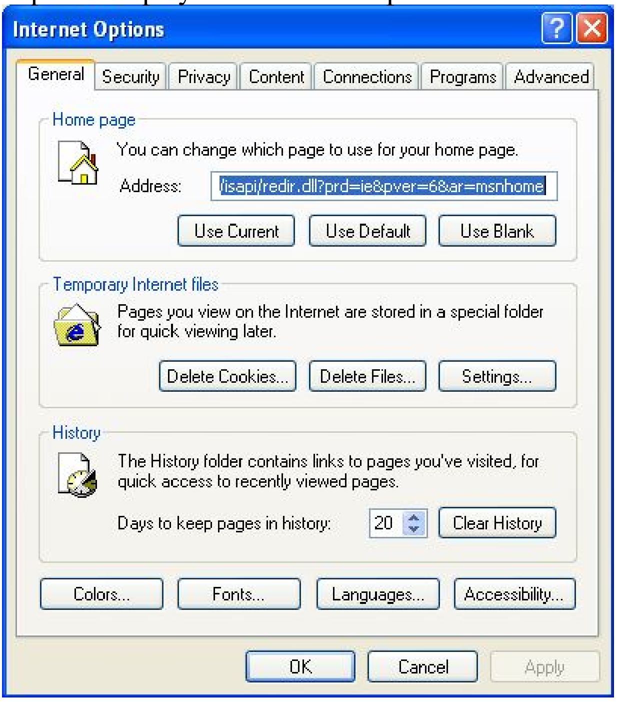
To configure Internet Explorer to use an HTTP proxy:

1. On the "Tools" menu, click "Internet Options":



Address: http://en.flossmanu

2. Internet Explorer displays the "Internet Options" window:



You can change which page to use for your home page.

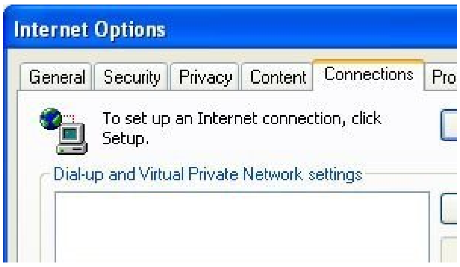
Address: /isapi/redir.dll?prd=ie&pver=6&ar=msnhome

Pages you view on the Internet are stored in a special folder for quick viewing later.

The History folder contains links to pages you've visited, for quick access to recently viewed pages.

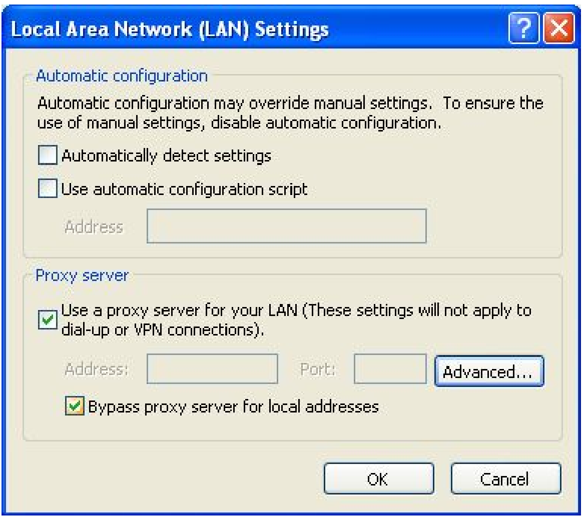
Days to keep pages in history: 20

3. Click the "Connections" tab.



To set up an Internet connection, click Setup.

4. Click "LAN Settings". The "Local Area Network (LAN) Settings" window



Automatic configuration may override manual settings. To ensure the use of manual settings, disable automatic configuration.

□ Automatically detect settings

□ Use automatic configuration script

Address

☑ Use a proxy server for your LAN (These settings will not apply to dial-up or VPN connections).

Address: Port:

☑ Bypass proxy server for local addresses

appears.

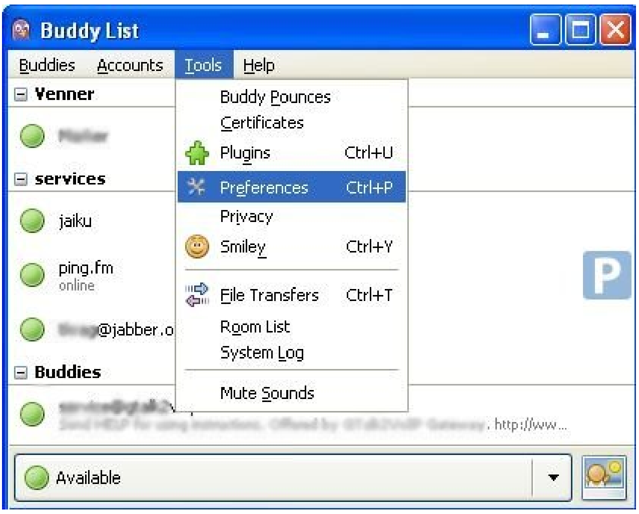
5. Select "Use a proxy server for your LAN".
6. Click "Advanced". The "Proxy Settings" window appears.
7. Enter the "Proxy address to use" and "Port" number in the first row of fields.
8. If you click the "Use the same proxy server for all protocols", Internet Explorer will attempt to send HTTPS (secure HTTP) and FTP traffic through the proxy. This may not work if you are using a public application proxy, since many of these do not support HTTPS and FTP traffic. If, on the other hand your HTTPS and/or FTP traffic is being blocked, you can try to find a public application proxy with HTTPS and/or FTP support, and use the "Use this proxy server for all protocols" setting in Internet Explorer.

Now Internet Explorer is configured to use an HTTP proxy.

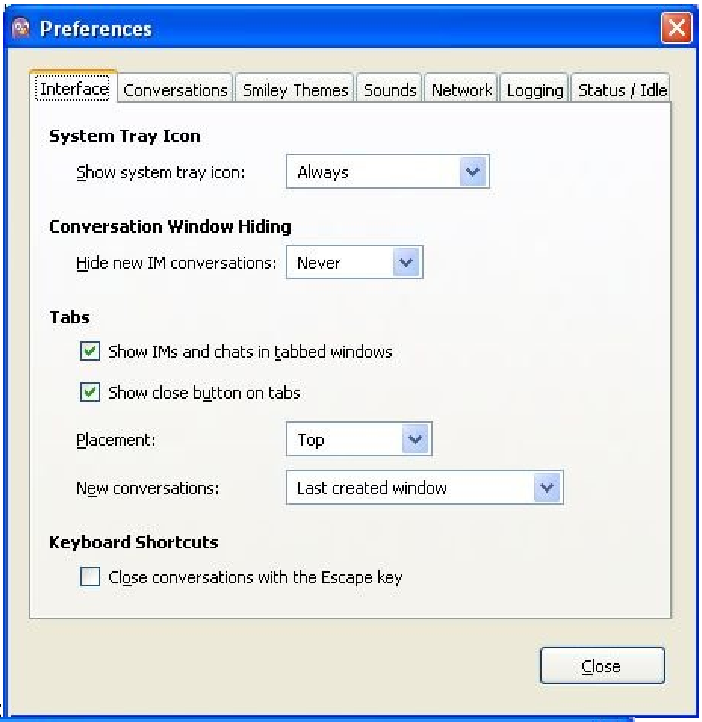
Pidgin Instant Messaging Client

Some Internet applications other than Web browsers can also use a HTTP proxy to connect to the Internet, potentially bypassing blocking. Here is an example with the instant messaging software Pidgin.

1. On the "Tools" menu, click "Preferences":



Pidgin displays the "Preferences" window:



System Tray Icon

Show system tray icon: Always

Conversation Window Hiding

Hide new IM conversations: Never

Tabs

☑ Show IMs and chats in tabbed windows

☑ Show close button on tabs

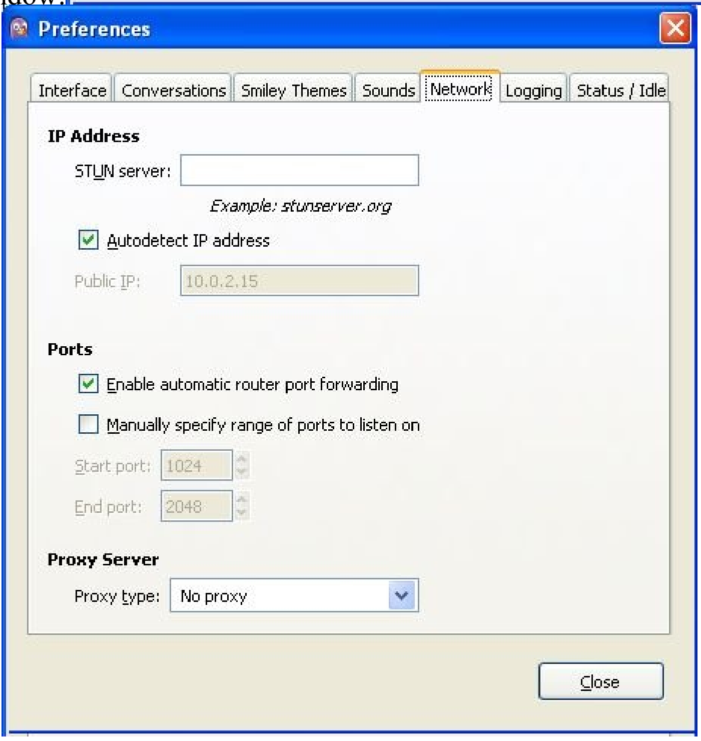
Placement: Top

New conversations: Last created window

Keyboard Shortcuts

☐ Close conversations with the Escape key

2. Click the "Network" tab to display it.



IP Address

STUN server:

Example: stunserver.org

☑ Autodetect IP address

Public IP: 10.0.2.15

Ports

☑ Enable automatic router port forwarding

☐ Manually specify range of ports to listen on

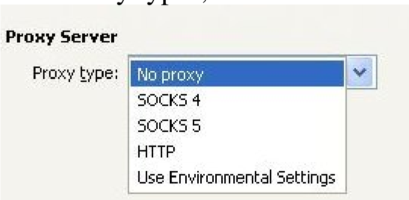
Start port: 1024

End port: 2048

Proxy Server

Proxy type: No proxy

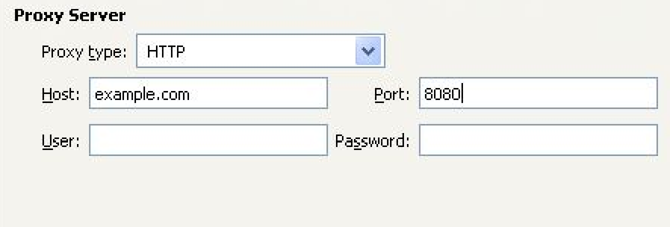
3. For "Proxy type", select "HTTP". Additional fields appear under that option.



Proxy Server

Proxy type: No proxy

4. Enter the "Host" address and "Port" number of your HTTP



Proxy Server

Proxy type: HTTP

Host: example.com

Port: 8080

User:

Password:

proxy.

5. Click "Close".

Pidgin is now configured to use the HTTP proxy.

When you're done with the proxy

When you are done using a proxy, particularly on a shared computer, return the settings you've changed to their previous values. Otherwise, those applications will continue to try to use the proxy. This could be a problem if you don't want people to know that you were using the proxy or if you were using a local proxy provided by a particular circumvention application that isn't running all the time.

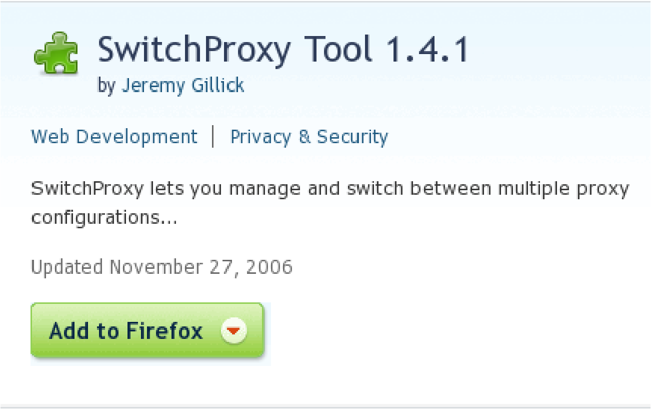
Installing SwitchProxy

SwitchProxy can switch between multiple **application proxy** configurations on any computer using the **Firefox** Web browser. This means it can easily run on **Windows**, **Linux** or **Mac OS X**.

SwitchProxy allows you to activate and deactivate proxy connections from a simple menu. It can also switch through a series of proxies at an interval you specify. (The author of SwitchProxy refers to this feature as support for "Anonymous" proxies, but using this feature does *not*, by itself, guarantee your anonymity!)

To install SwitchProxy:

1. Go to the web page for the SwitchProxy add-on for FireFox: https://addons.mozilla.org/en-US/firefox/addon/125

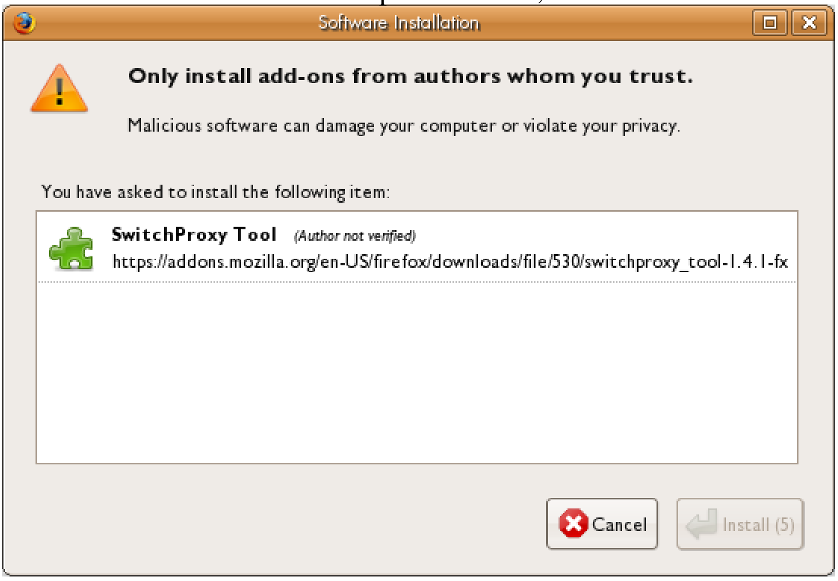


SwitchProxy Tool 1.4.1
by Jeremy Gillick

SwitchProxy lets you manage and switch between multiple proxy configurations...

Updated November 27, 2006

2. Click "Add to Firefox". The installation process starts, and this window appears:



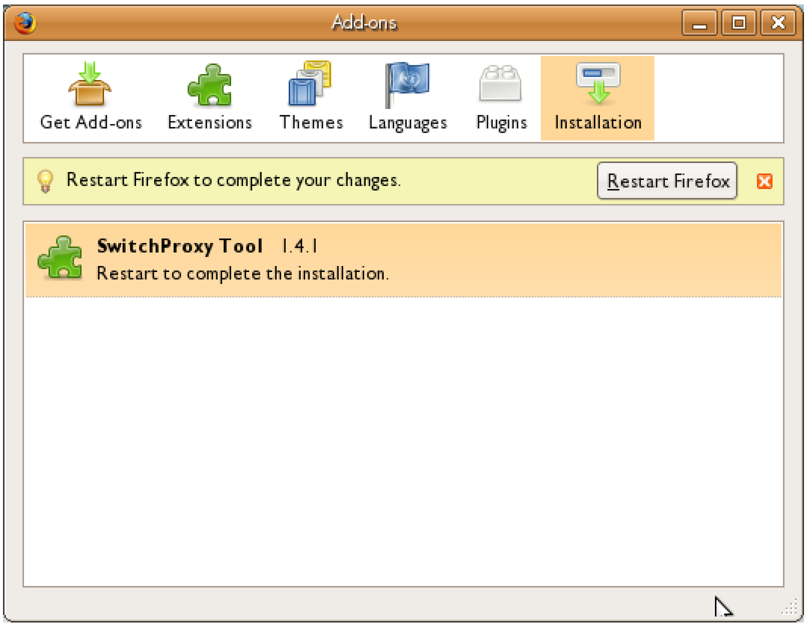
Only install add-ons from authors whom you trust.

Malicious software can damage your computer or violate your privacy.

You have asked to install the following item:

SwitchProxy Tool (Author not verified)
https://addons.mozilla.org/en-US/firefox/downloads/file/530/switchproxy_tool-1.4.1-fx

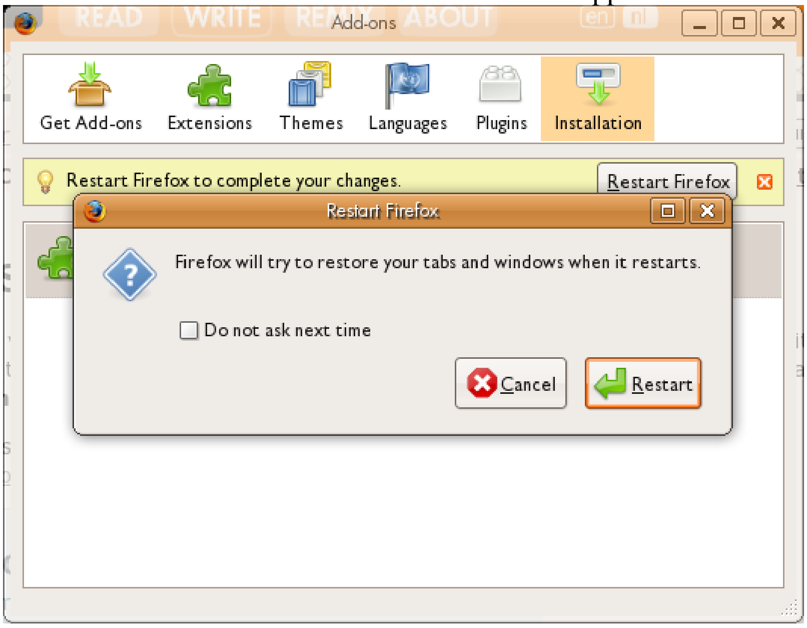
3. If you click on this window, the "Install" button (which is initially inactive) counts down from 5 to 1. Then the "Install" button becomes active.
4. Click "Install". The add-on downloads automatically and installs itself. The following window appears:



Restart Firefox to complete your changes.

SwitchProxy Tool 1.4.1
Restart to complete the installation.

5. Click "Restart Firefox". A confirmation window appears:



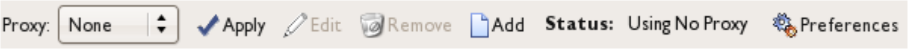
Restart Firefox to complete your changes.

Firefox will try to restore your tabs and windows when it restarts.

□ Do not ask next time

6. Click "Restart". Firefox shuts down and then re-opens.

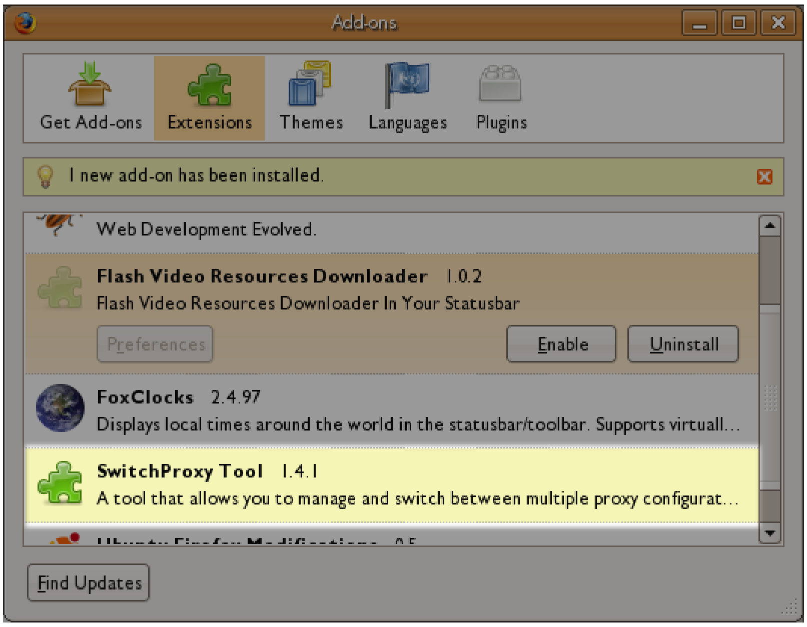
After you install the SwitchProxy add-on, the Firefox Toolbar shows tools for SwitchProxy:



Proxy: None

Status: Using No Proxy

The Firefox "Add-ons" window shows that SwitchProxy has been installed:



1 new add-on has been installed.

Web Development Evolved.

Flash Video Resources Downloader 1.0.2
Flash Video Resources Downloader In Your Statusbar

FoxClocks 2.4.97
Displays local times around the world in the statusbar/toolbar. Supports virtuall...

SwitchProxy Tool 1.4.1
A tool that allows you to manage and switch between multiple proxy configurat...

The list of Add-ons will vary from what is shown here. Scroll down until you see the SwitchProxy tool. If you click on "SwitchProxy Tool", you can access the Preference controls.

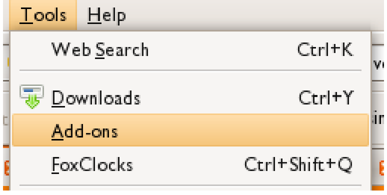
Congratulations! The SwitchProxy tool should now be installed. Now you need to learn how to configure and use it.

Using Switch Proxy

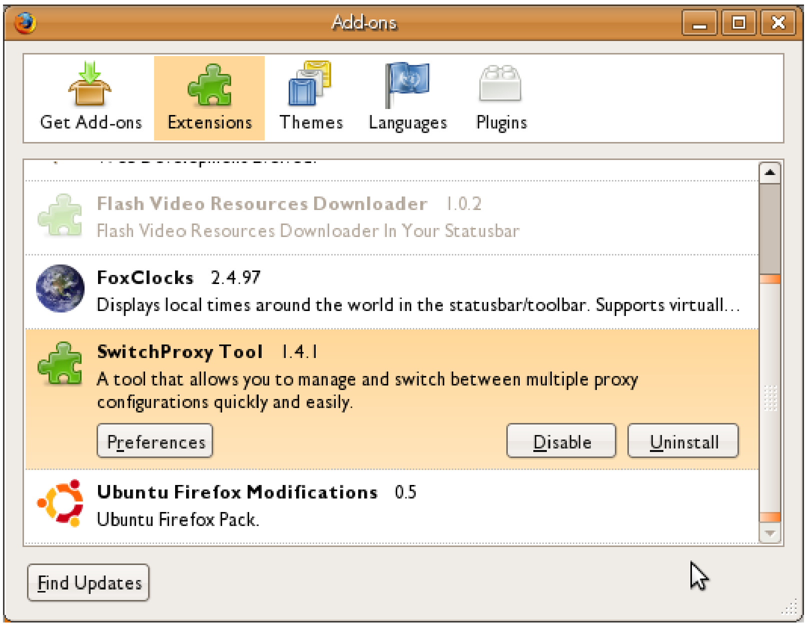
SwitchProxy lets you quickly change the proxy settings of your Firefox browser. You can do this in order to use a **public proxy** available to everyone, a specific **private proxy** to which you've arranged access, or a **local proxy** provided by a client application such as SSH. Usually, you will need to have a particular application proxy or list of application proxies that you want to use *before* using SwitchProxy; SwitchProxy mainly helps you use proxies, not find them. SwitchProxy also supports loading a list of several proxies and switching frequently among them.

SwitchProxy configuration

To configure SwitchProxy, you need to open its configuration window, accessed through the Firefox "Tools" menu:



Choose "Add-ons". You should see "SwitchProxy Tool" listed in the Add-ons menu. Click the link once to reveal the "Preferences" button:



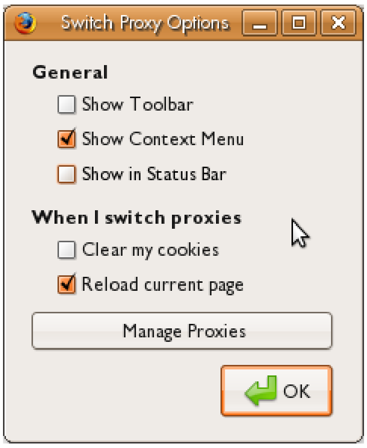
Flash Video Resources Downloader 1.0.2
Flash Video Resources Downloader In Your Statusbar

FoxClocks 2.4.97
Displays local times around the world in the statusbar/toolbar. Supports virtuall...

SwitchProxy Tool 1.4.1
A tool that allows you to manage and switch between multiple proxy configurations quickly and easily.

Ubuntu Firefox Modifications 0.5
Ubuntu Firefox Pack.

Click the "Preferences" button to display the panel for setting a simple set of preferences:



General
- ☐ Show Toolbar
- ☑ Show Context Menu
- ☐ Show in Status Bar

When I switch proxies
- ☐ Clear my cookies
- ☑ Reload current page

The items in the **General** section relate only to where SwitchProxy information will be displayed in the Browser.

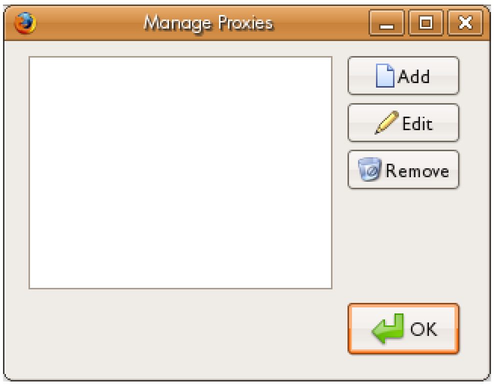
The second section (**When I switch proxies**) is more important, as this determines how SwitchProxy will behave. When you switch proxies, SwitchProxy can do a number of things. It can automatically clear your Cookies and it can reload the page that you were using through the new proxy. These behaviors are controlled by the check boxes displayed.

You should choose "Clear my cookies" when reloading a proxy, as some sites might be able to correlate your previous **IP address** with a cookie. Reloading the page automatically when you change a proxy will ensure there no is communication still taking place through the old proxy settings.

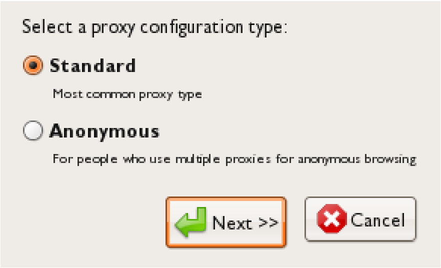
You manage the core of SwitchProxy's functionality with the last button, "Manage Proxies". If you click this button you can add, edit and remove proxies.

Adding a Basic Proxy

Let's add a proxy to SwitchProxy. To do this, we need to first choose "Manage Proxies" above. The "Mange Proxies" window appears:



If you had other proxies already configured inside SwitchProxy, they would be displayed here. To add a new proxy, click "Add":



Select a proxy configuration type:

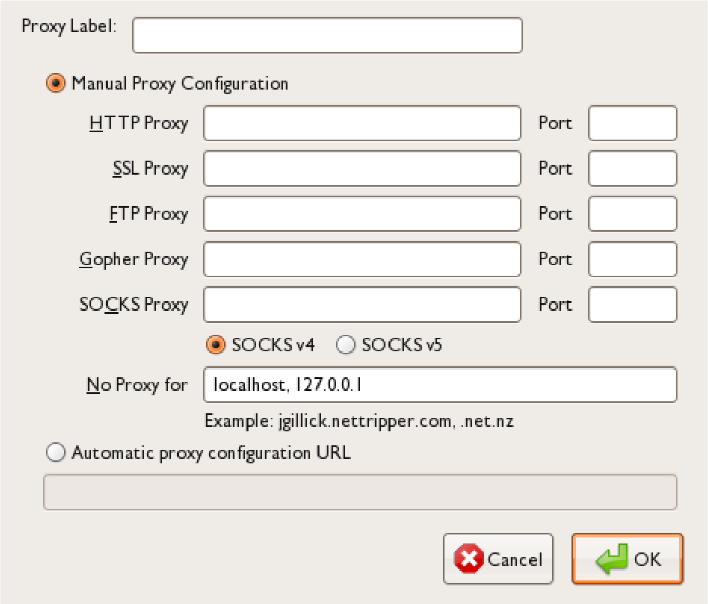
● **Standard**
Most common proxy type

○ **Anonymous**
For people who use multiple proxies for anonymous browsing

Choosing **Standard** allows you set up a proxy for Web browsing, uploading files, and other typical actions. This is useful for accessing servers that might be blocked.

SwitchProxy also offers an **Anonymous** option; however, this option is misnamed because it does not guarantee anonymity. It simply allows the use of multiple proxies with frequent switching among them.

Standard Proxy Settings



Proxy Label:

● Manual Proxy Configuration

HTTP Proxy Port

SSL Proxy Port

FTP Proxy Port

Gopher Proxy Port

SOCKS Proxy Port

● SOCKS v4 ○ SOCKS v5

No Proxy for: localhost, 127.0.0.1

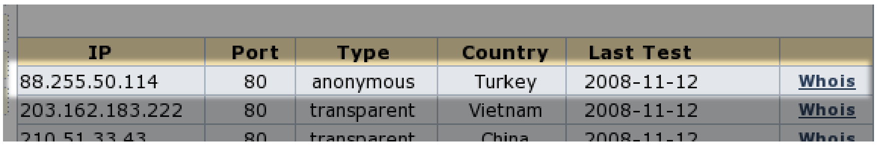
Example: jgillick.nettripper.com, .net.nz

○ Automatic proxy configuration URL

You need to know the settings for the proxy you wish to add. This can be quite a lot of information depending on what type of access you require and how the proxy manages that type of access.

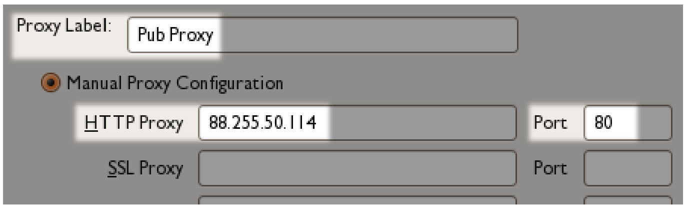
Ideally, you should already know the settings for the proxies you want to try to use with SwitchProxy. For purposes of example, we will find a **public proxy** from the "Public Proxy Servers" web site (http://www.publicproxyservers.com) and add it to SwitchProxy. (We have no information about who operates these proxies, so we don't really know how trustworthy they are.)

First, on the Public Proxy Servers main page, we choose "proxy list [1]" from the left-hand navigation panel (http://www.publicproxyservers.com/page1.html). We then see a list:



IP	Port	Type	Country	Last Test	
88.255.50.114	80	anonymous	Turkey	2008-11-12	Whois
203.162.183.222	80	transparent	Vietnam	2008-11-12	Whois
210.51.33.43	80	transparent	China	2008-11-12	Whois

We'll enter the **IP** (in this case, 88.255.50.114) and **Port** (in this case, 80) information from the list into the first fields of the Standard configuration window:



Proxy Label: Pub Proxy

● Manual Proxy Configuration

HTTP Proxy 88.255.50.114 Port 80

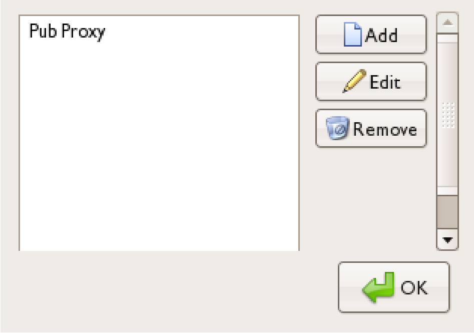
SSL Proxy Port

You can give each proxy a label (we are using "Pub Proxy" in the example). This is all you need to do to set up this proxy. If you want to set up the proxy for other types of access (SSL, FTP, Gopher or Socks), you would need to continue filling out the details in the other fields. Usually the port and IP settings are the same, so you would use the same details for each type of access required.

Note:

1. Many proxies only offer HTTP (Web browsing) access. If you want to use a proxy for other types of Internet use, you can try it to see if it works.
2. Many open proxies only work for a few hours at a time, so be prepared to switch among several to find one that is working.
3. The settings are only used by the Firefox browser using SwitchProxy. If you open another browser or use another type of application (for example, an FTP client), it does not have access to the SwitchProxy settings.

After you enter the details, click "OK" to save the settings. The "Manage Proxies" window appears again:



Pub Proxy

Click "OK" again to close this window and save the new proxy to your list. It is important to note that these proxy settings are not active until you *make* the proxy active through SwitchProxy.

Adding a list of proxies for automated switching

SwitchProxy also allows you to create a list of proxies and to set an interval for automatically switching between them. This option is confusingly referred to as "Anonymous" proxy configuration, though, in reality, it does not guarantee anonymity.

If you decide to use this feature, you can set the proxy list yourself. It will be a plain text file with a format like this:

```
193.147.162.166:3124
133.1.74.162:3124
130.75.87.83:3124
128.112.139.80:3128
128.112.139.80:3124
72.36.112.74:3124
199.26.254.65:3124
```

The format of each line is simply

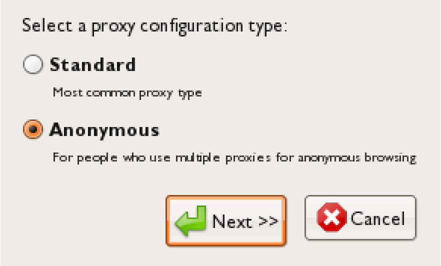
IP address:Port number

It is important to place the colon between the two numbers and not to include "http://" before the IP address of the proxy. Each proxy must be on a separate line and the file must be formatted as a text file (sometimes called a .txt file) and **not** a word processor file (such as a Microsoft Word .doc file or OpenOffice .odt file).

There are also services online that provide public proxy lists compatible with this feature. Although these services are themselves blocked in some places, you may be able to find useful public proxy lists through a Web search.

For instance, a quick search for "switchproxy anonymous proxy lists" in Google recently led to this site: http://www.shroomery.org/ythan/proxylist.php. This service, provided by someone with an interest in this area (apparently an amateur, not a commercial service) takes a list of proxies from XROXY (http://www.xroxy.com/proxylist.php?type=Anonymous) and formats the list so that SwitchProxy can use it.

You can add any of these lists -- a list you produce, or an online list -- to SwitchProxy's configuration as a set of "Anonymous" proxies. To do this, choose the "Anonymous" settings option instead of the "Standard" configuration setting.

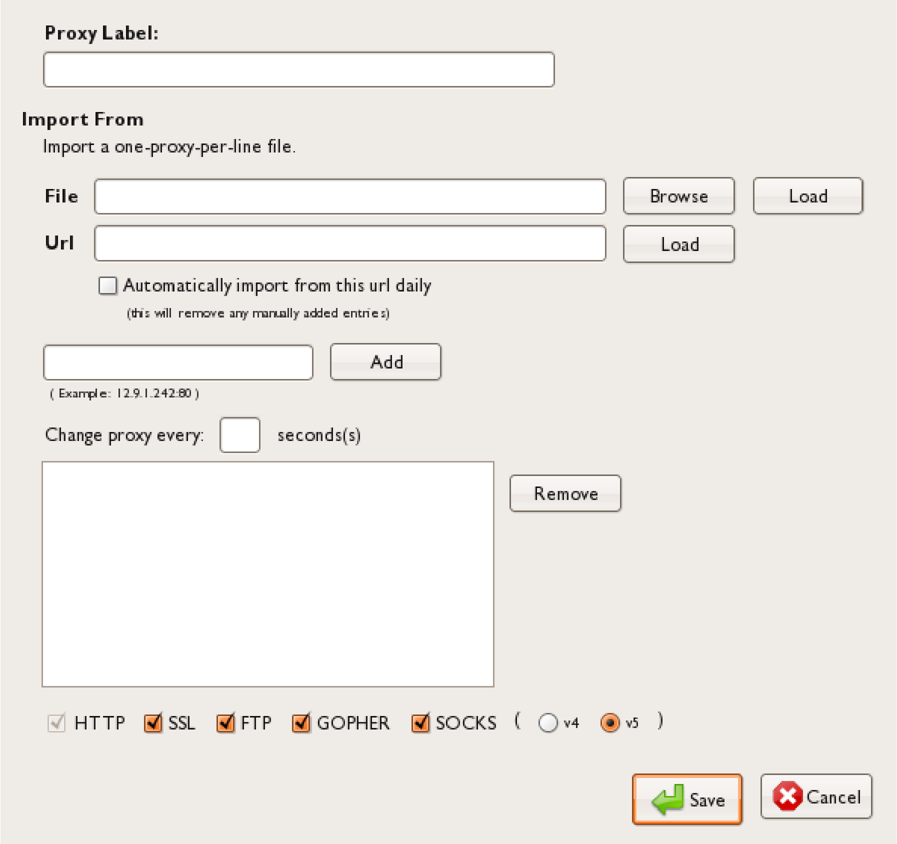


Select a proxy configuration type:

○ **Standard**
Most common proxy type

● **Anonymous**
For people who use multiple proxies for anonymous browsing

Click "Next >>" and the settings window appears:



Proxy Label:

Import From
Import a one-proxy-per-line file.

File

Url

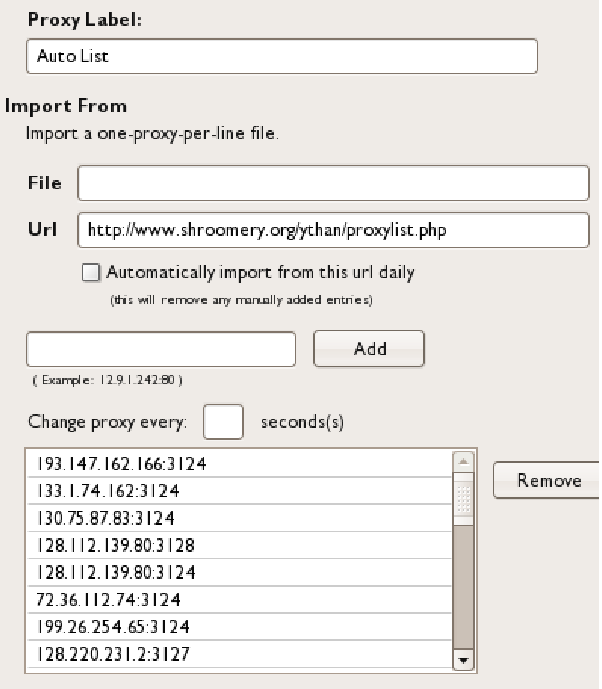
□ Automatically import from this url daily
(this will remove any manually added entries)

(Example: 12.9.1.242:80)

Change proxy every: seconds(s)

☑ HTTP ☑ SSL ☑ FTP ☑ GOPHER ☑ SOCKS (○ v4 ● v5)

To use the online list, simply enter the URL of the list into the **Url** field and click "Load". To add a list you have created you must click "Browse" next to the **File** field, select the file from your computer's hard drive and then click "Load". Don't forget to give the list a name (or "Label"). For example, using the online list mentioned in the example above gave this result after clicking "Load":



Proxy Label: Auto List

Import From

Import a one-proxy-per-line file.

File

Url http://www.shroomery.org/ythan/proxylist.php

□ Automatically import from this url daily

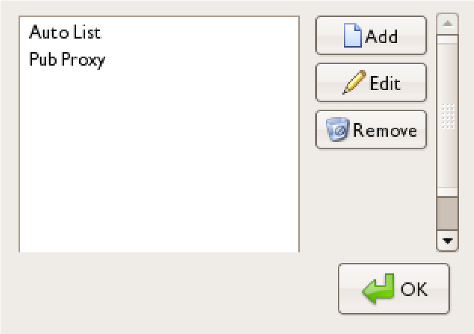
(this will remove any manually added entries)

(Example: 12.9.1.242:80)

Change proxy every: seconds(s)

```
193.147.162.166:3124
133.1.74.162:3124
130.75.87.83:3124
128.112.139.80:3128
128.112.139.80:3124
72.36.112.74:3124
199.26.254.65:3124
128.220.231.2:3127
```

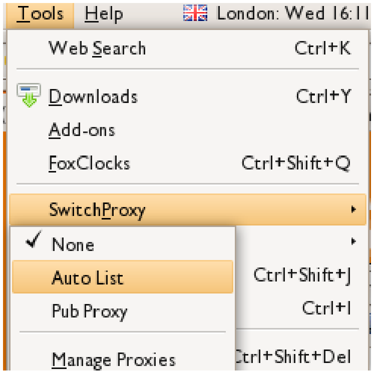
Now you must choose the interval for cycling through the proxies. Intervals for automatic switching in SwitchProxy are represented in seconds, so if you want to set an interval of 3 minutes, you would type "180" into the "Change proxy every[ ]" field. After you click "OK", the window closes and SwitchProxy saves your new proxy list:



Auto List
Pub Proxy

Using SwitchProxy

To use the proxies you have saved, just click the "Tools" menu in Firefox:



Selecting "SwitchProxy", you should see a list of proxies you have already configured. Selecting one of them activates that proxy item. To use no proxies choose "None".

Disadvantages and Risks

Using a public application proxy does *not* guarantee that you will be anonymous. Whenever you use any proxy, you are trusting the operator of the proxy not to reveal or abuse information about you or how you use the proxy.

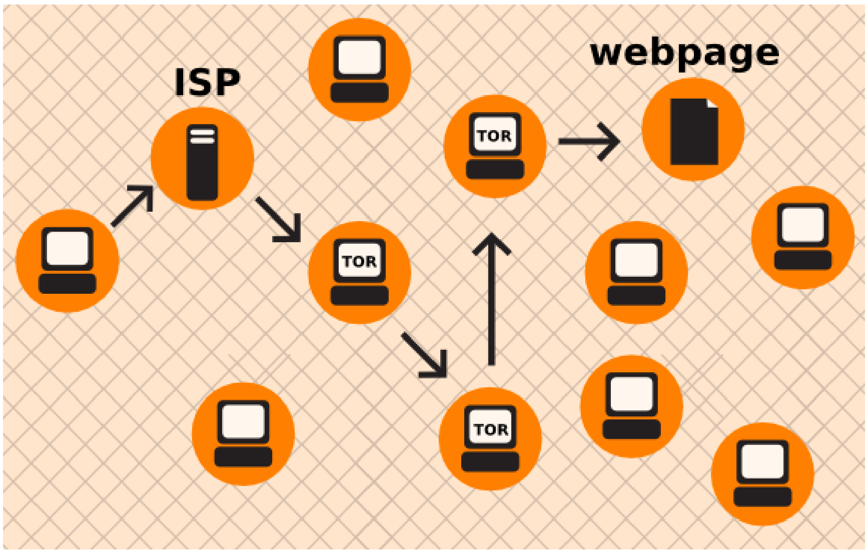
Your communications with the proxy can also be observed by a network operator. If you visit a Web site on different occasions using the same computer, for instance, the site can potentially recognize you as the same person by using mechanisms like cookies -- even if you use different proxy settings for each visit.

Although Tor provides a local application proxy, you should not use SwitchProxy to activate Tor. Use Torbutton instead. Torbutton protects you against a variety of potential privacy risks (such as **DNS leaks**) that SwitchProxy does not.

Tor - The Onion Router

Tor (The Onion Router) is a very sophisticated network of proxy servers.

When you are using Tor to access a Web site, your communications are randomly routed through a network of independent, volunteer proxies. All the traffic between Tor servers (or relays) is encrypted, and each of the relays knows only the IP address of two other relays -- the one immediately previous to it and the one immediately after it in the chain.



This makes it very difficult for:

- your ISP to know what your target Web site is or what information you are sending
- the target Web site to know who you are (at least, to know your IP address)
- any of the independent relays to know who you are and where you go

What do I need to use the Tor network?

To connect to the Internet through the Tor network and use it for **anonymity** and **circumvention**, you need to install the Tor client software on your computer. (It is also possible to run a portable version of the program from a memory stick or other external device.)

Tor is compatible with most versions of **Windows, Mac OS X and GNU/Linux**.

With what software is Tor compatible?

Tor uses a SOCKS proxy interface to connect to applications, so any application that supports SOCKS (versions 4, 4a and 5) can be anonymized using Tor, including:

- most Web browsers
- many instant messaging and IRC clients
- SSH clients
- e-mail clients

If you installed Tor from the **Tor Bundle**, **Browser Bundle** or **IM Browser Bundle**, Tor also configured an http application proxy as a frontend to the Tor network. This will allow some applications that do not support SOCKS to work with Tor.

If you are mostly interested in using Tor for Web surfing and chatting, you may find it easiest to use the **Tor Browser Bundle** or the **Tor IM Browser Bundle** which will provide you with ready-to-use pre-configured solutions. The Tor browser bundle also includes Torbutton, which improves privacy protection when using Tor with a Web browser. Both versions of Tor can be downloaded at http://www.torproject.org/torbrowser/index.html.en.

Advantages and Risks

Tor can be a very effective tool for circumvention and protecting your identity. Tor's encryption hides the contents of your communications from your local network operator, and conceals whom you are communicating with or what Web sites you're viewing. When used properly, it provides significantly stronger anonymity protection than a single proxy.

- But Tor is vulnerable to blocking. Most Tor nodes are listed in a public directory, so it is easy for network operators to access the list and add the IP addresses of nodes to a filter. (One way of attempting to get around this kind of blocking is to use one of several **Tor bridges**, which are Tor nodes not publicly listed, specifically to avoid blocking.)
- Some programs you might use with Tor have problems that can compromise anonymity.
- Also, if you're not using additional encryption to protect your communications, your data will be unencrypted once it reaches the last Tor node in the chain (called an **exit node**). This means that your data will be potentially visible to the owner of the last Tor node and to the ISP between that node and your destination Web site.

The developers of Tor have thought a lot about these and other risks and offer three warnings:

1. Tor does not protect you if you do not **use it correctly**. Read the list of warnings here: http://www.torproject.org/download.html.en#Warning, and then make sure to follow the instructions for your platform carefully: http://www.torproject.org/documentation.html.en#RunningTor

2. Even if you configure and use Tor correctly, there are still **potential attacks** that could compromise Tor's ability to protect you: https://wiki.torproject.org/noreply/TheOnionRouter/TorFAQ#RemainingAttacks

3. **No anonymity system is perfect** these days, and Tor is no exception: you should not rely solely on the current Tor network if you really need strong anonymity.

Using Tor Browser Bundle

The Tor Browser Bundle lets you use Tor on Windows without requiring you to configure a Web browser. Even better, it's also a portable application that can be run from a USB flash drive, allowing you to carry it to any Windows PC without installing it on each computer's hard drive.

Downloading Tor Browser Bundle

You can download the Tor Browser Bundle from the torproject.org Web site, either as a single file (13MB) or a "split" version that is multiple files of 1.4 MB each. If your Internet connection is slow and unreliable, the split version may work better than trying to download one very large file.

If the torproject.org Web site is filtered from where you are, type "tor mirrors" in your favorite Web search engine: The results probably include some alternative addresses to download the Tor Browser Bundle.

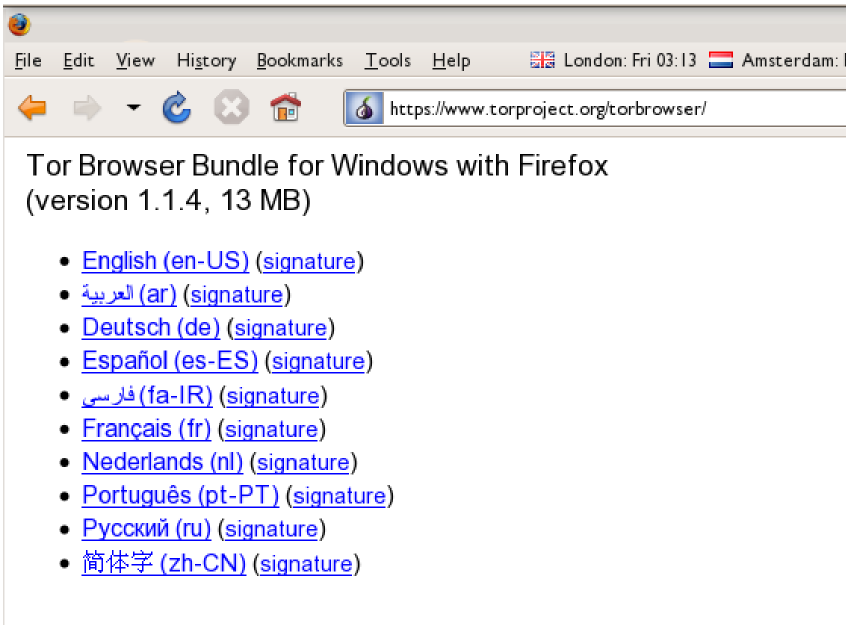
Caution: When you download Tor Bundle (plain or split versions), you should check the signatures of the files, especially if you are downloading the files from a mirror site. This step ensures that the files have not been tampered with. To learn more about signature files and how to check them, read https://wiki.torproject.org/noreply/TheOnionRouter/VerifyingSignatures

(You can also download the GnuPG software that you will need to check the signature here: http://www.gnupg.org/download/index.en.html#auto-ref-2)

The instructions below refer to installing Tor Browser on Microsoft Windows. If you are using a different operating system, refer to the torproject.org website for download links and instructions.

Installing from a single file

1. In your Web browser, enter the download URL for Tor Browser:

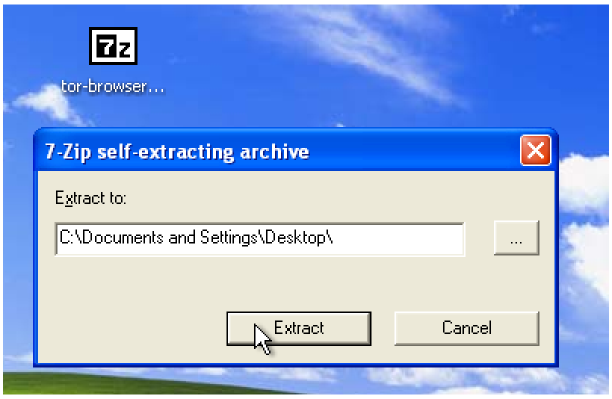


Tor Browser Bundle for Windows with Firefox (version 1.1.4, 13 MB)

- English (en-US) (signature)
- العربية (ar) (signature)
- Deutsch (de) (signature)
- Español (es-ES) (signature)
- فارسی (fa-IR) (signature)
- Français (fr) (signature)
- Nederlands (nl) (signature)
- Português (pt-PT) (signature)
- Русский (ru) (signature)
- 简体字 (zh-CN) (signature)

   https://www.torproject.org/torbrowser/

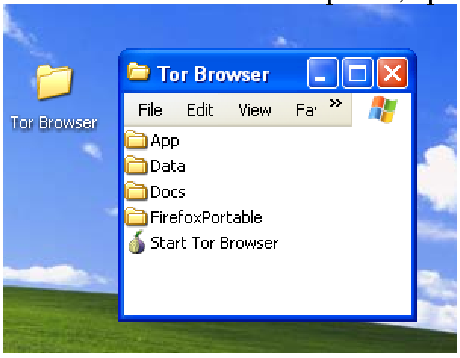
2. Click the link for your language to download the installation file.
3. Double-click the .EXE file you just downloaded. A "7-Zip self-extracting archive" window appears.


tor-browser...
7-Zip self-extracting archive
Extract to:
C:\Documents and Settings\Desktop\
...
Extract
Cancel

4. Choose a folder into which you want to extract the files and click "Extract".

   Note: You can choose to extract the files directly onto a USB key or memory stick if you want to use Tor Browser on different computers (for instance on public computers in Internet cafÃ©s).

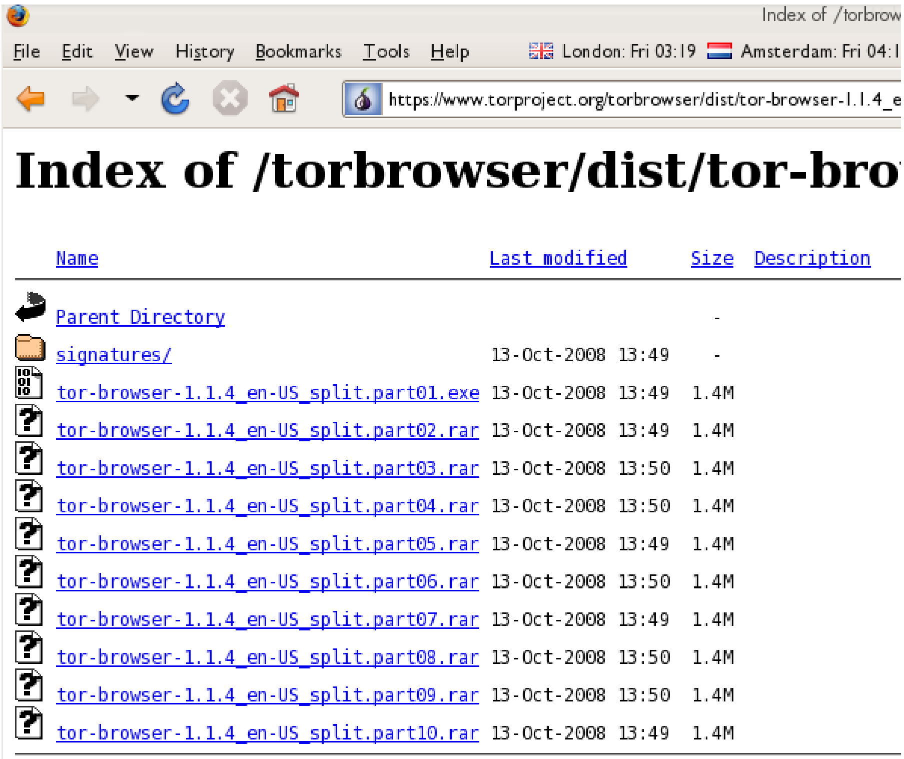
5. When the extraction is completed, open the folder and check that the contents match the image below:



6. To clean up, delete the .EXE file you originally downloaded.

Installing from split files

1. In your Web browser, enter the URL for the split version of the Tor Browser Bundle (https://www.torproject.org/torbrowser/split.html), then click the link for your language to get to a page that looks like the one for English below:

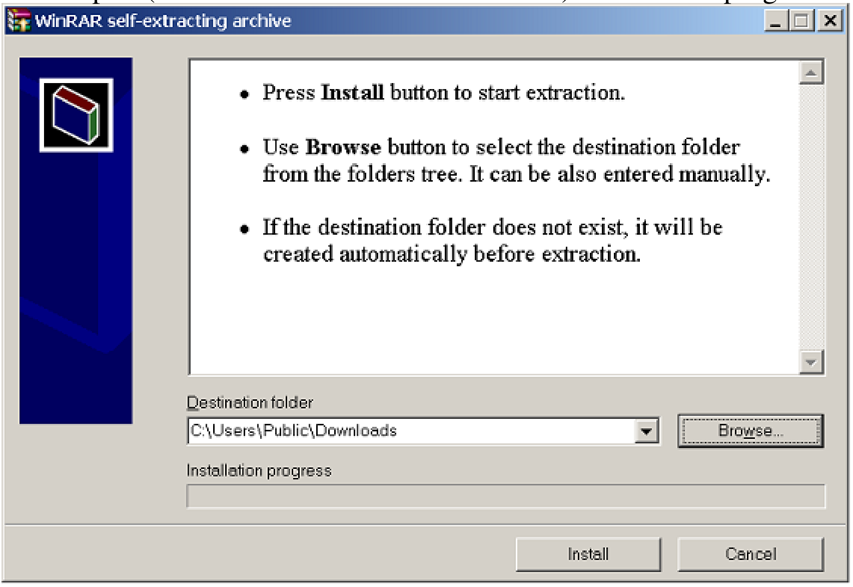


https://www.torproject.org/torbrowser/dist/tor-browser-1.1.4_e

Index of /torbrowser/dist/tor-bro

Name	Last modified	Size	Description
Parent Directory		-	
signatures/	13-Oct-2008 13:49	-	
tor-browser-1.1.4_en-US_split.part01.exe	13-Oct-2008 13:49	1.4M	
tor-browser-1.1.4_en-US_split.part02.rar	13-Oct-2008 13:49	1.4M	
tor-browser-1.1.4_en-US_split.part03.rar	13-Oct-2008 13:50	1.4M	
tor-browser-1.1.4_en-US_split.part04.rar	13-Oct-2008 13:50	1.4M	
tor-browser-1.1.4_en-US_split.part05.rar	13-Oct-2008 13:49	1.4M	
tor-browser-1.1.4_en-US_split.part06.rar	13-Oct-2008 13:50	1.4M	
tor-browser-1.1.4_en-US_split.part07.rar	13-Oct-2008 13:49	1.4M	
tor-browser-1.1.4_en-US_split.part08.rar	13-Oct-2008 13:50	1.4M	
tor-browser-1.1.4_en-US_split.part09.rar	13-Oct-2008 13:50	1.4M	
tor-browser-1.1.4_en-US_split.part10.rar	13-Oct-2008 13:49	1.4M	

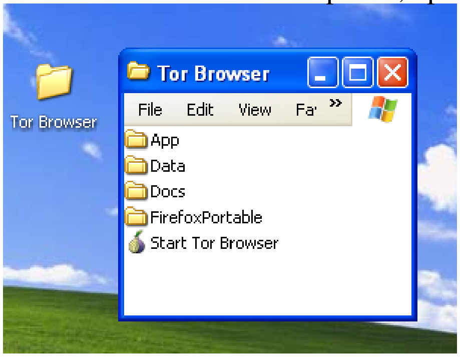
2. Click each file to download it (one ending in ".exe" and nine others ending in ".rar"), one after the other, and save them all in one folder on your hard drive.
3. Double-click the first part (the file whose name ends in ".exe"). This runs a program to gather all the parts together.



- Press **Install** button to start extraction.
- Use **Browse** button to select the destination folder from the folders tree. It can be also entered manually.
- If the destination folder does not exist, it will be created automatically before extraction.

Destination folder: C:\Users\Public\Downloads

4. Choose a folder where you want to install the files, and click "Install". The program displays messages about its progress while it's running, and then quits.
5. When the extraction is completed, open the folder and check that the contents match the image below:



6. To clean up, delete all the files you originally downloaded.

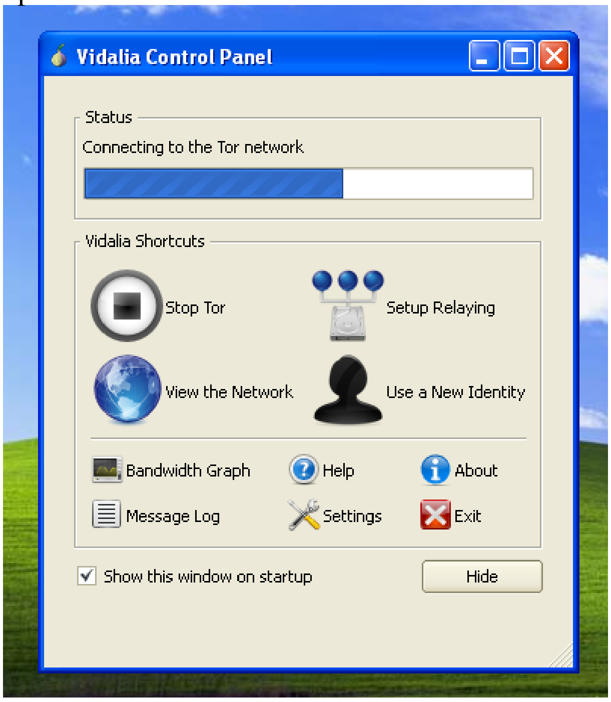
Using Tor Browser

Before you start:

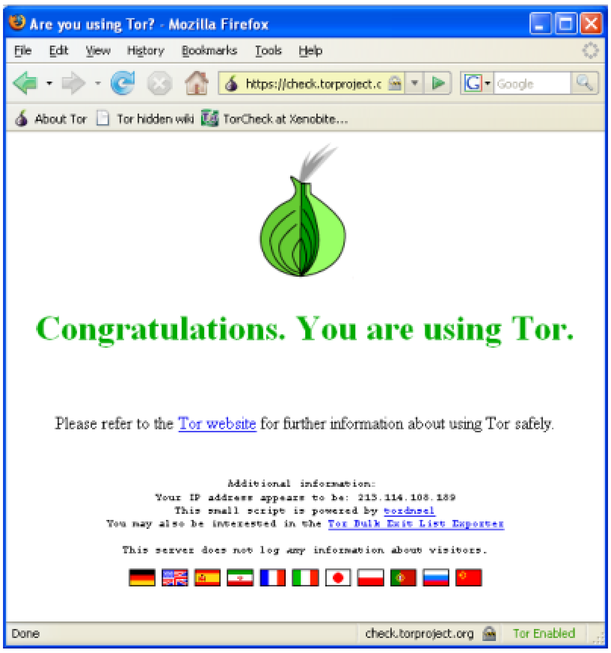
- **Close Firefox.** If Firefox is installed on your computer, make sure it is not currently running.
- **Close Tor.** If Tor is already installed on your computer, make sure it is not currently running.

Launch Tor Browser:

- In the "Tor Browser" folder, double-click "Start Tor Browser". The Tor control panel ("Vidalia") opens and Tor starts to connect to the Tor network.



When a connection is established, Firefox automatically connects to the TorCheck page and then confirms if you are connected to the Tor network. This may take some time, depending on the quality of your Internet connection.



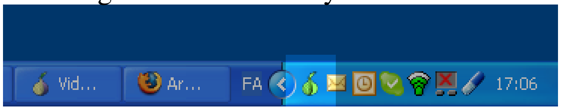
Congratulations. You are using Tor.

Please refer to the Tor website for further information about using Tor safely.

Additional information:
Your IP address appears to be: 213.114.108.189
This small script is powered by tordnsel
You may also be interested in the Tor Bulk Exit List Exporter

This server does not log any information about visitors.

If you are connected to the Tor network, a green onion icon appears in the System Tray on the lower-right-hand corner of your screen:

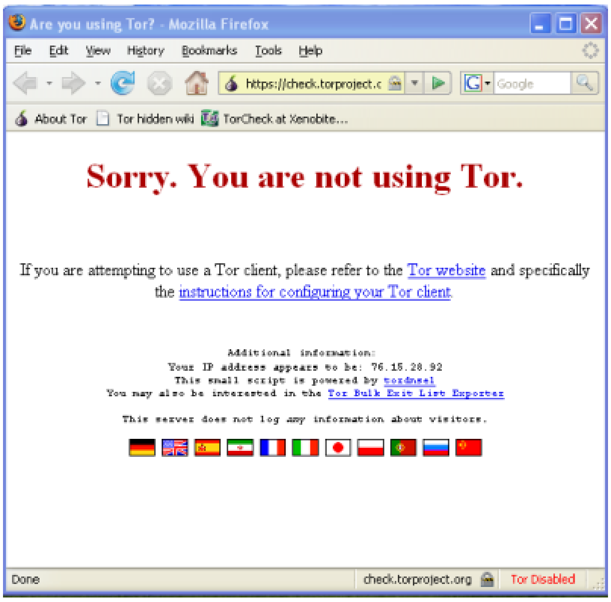


Browsing the Web using Tor Browser

Try viewing a few Web sites, and see whether they display. The sites are likely to load more slowly than usual because your connection is being routed through several relays.

If this does not work

If the onion in the Vidalia Control Panel never turns green or if Firefox opened, but displayed a page saying "Sorry. You are not using Tor", as in the image below, then you are not using Tor.



Sorry. You are not using Tor.

If you are attempting to use a Tor client, please refer to the Tor website and specifically the instructions for configuring your Tor client.

Additional information:
Your IP address appears to be: 76.15.28.92
This small script is powered by tordnsel
You may also be interested in the Tor Bulk Exit List Exporter

This server does not log any information about visitors.

If you see this message, close Firefox and Tor Browser and then repeat the steps above. You can perform this check to ensure that you are using tor, at any time by clicking the bookmark button labelled "TorCheck at Xenobite..." in the Firefox toolbar.

If Firefox browser does not launch, another instance of the browser may be interfering with Tor Browser. To fix this:

1. Open the Windows Task Manager. How you do this depends on how your computer is set up. On most systems, you can right-click in the Task Bar and then click "Task Manager".
2. Click the "Processes" tab.
3. Look for a process in the list named "firefox.exe".
4. If you find one, select the entry and click "End Process".
5. Repeat the steps above to launch Tor Browser.

If Tor Browser still doesn't work after two or three tries, Tor may be partly blocked by your ISP and you should try using the **bridge** feature of Tor.

Alternatives

There are two other projects that bundle Tor and a browser:

- XeroBank, a bundle of Tor with Firefox (http://xerobank.com/xB_Browser.php)
- OperaTor, a bundle of Tor with Opera (http://archetwist.com/en/opera/operator)

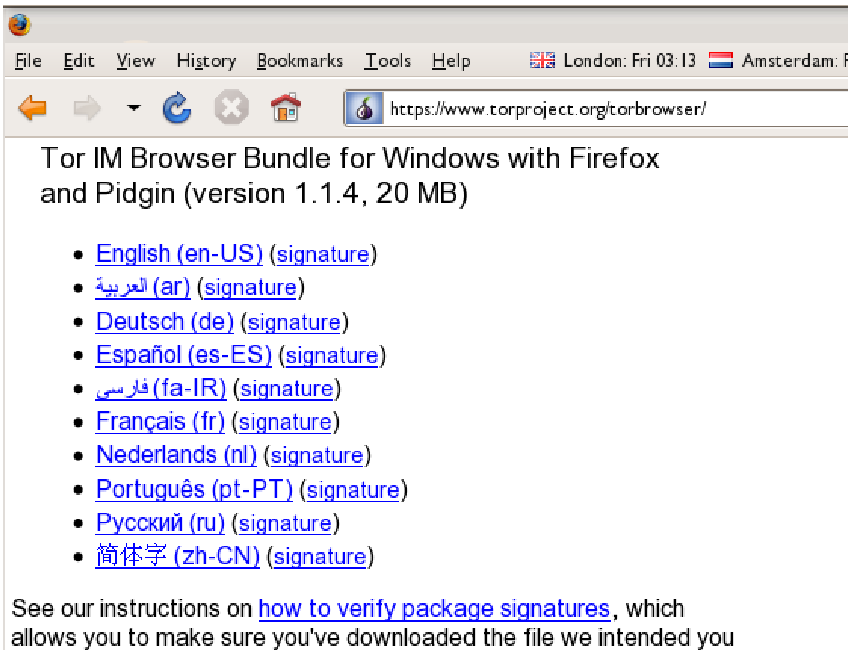
Using Tor IM Browser Bundle

The **Tor IM Browser Bundle** is similar to the **Tor Browser Bundle**, but offers you access to the **Pidgin** multi-protocol Instant Messaging client, so you can chat encrypted over your favourite Instant Messenger protocol like ICQ, MSN Messenger, Yahoo! Messenger or QQ which may be filtered.

You can learn more about Pidgin here: http://www.pidgin.im/

Download Tor IM Browser Bundle

You can download the Tor IM Browser Bundle directly from the Tor Web site (20MB) at https://www.torproject.org/torbrowser/

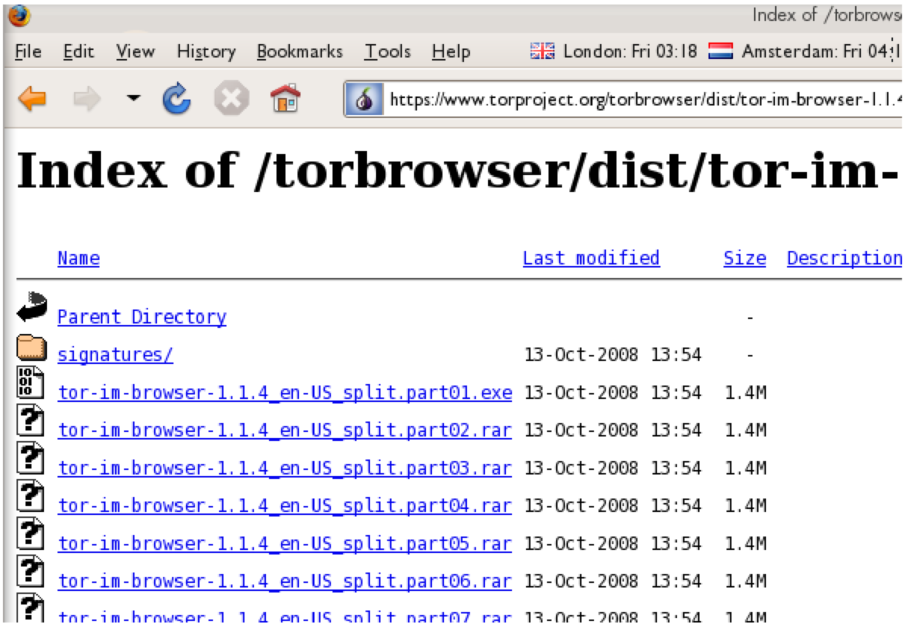

File Edit View History Bookmarks Tools Help
London: Fri 03:13
Amsterdam: F
https://www.torproject.org/torbrowser/

Tor IM Browser Bundle for Windows with Firefox and Pidgin (version 1.1.4, 20 MB)

- English (en-US) (signature)
- العربية (ar) (signature)
- Deutsch (de) (signature)
- Español (es-ES) (signature)
- فارسی (fa-IR) (signature)
- Français (fr) (signature)
- Nederlands (nl) (signature)
- Português (pt-PT) (signature)
- Русский (ru) (signature)
- 简体字 (zh-CN) (signature)

See our instructions on how to verify package signatures, which allows you to make sure you've downloaded the file we intended you

(If your Internet connection is slow or unreliable, you can also get a **split up version** on the torproject.org Web site at https://www.torproject.org/torbrowser/split.html).


Index of /torbrows
File Edit View History Bookmarks Tools Help
London: Fri 03:18
Amsterdam: Fri 04:
https://www.torproject.org/torbrowser/dist/tor-im-browser-1.1.4

Index of /torbrowser/dist/tor-im-

Name	Last modified	Size	Description
Parent Directory		-	
signatures/	13-Oct-2008 13:54	-	
tor-im-browser-1.1.4_en-US_split.part01.exe	13-Oct-2008 13:54	1.4M	
tor-im-browser-1.1.4_en-US_split.part02.rar	13-Oct-2008 13:54	1.4M	
tor-im-browser-1.1.4_en-US_split.part03.rar	13-Oct-2008 13:54	1.4M	
tor-im-browser-1.1.4_en-US_split.part04.rar	13-Oct-2008 13:54	1.4M	
tor-im-browser-1.1.4_en-US_split.part05.rar	13-Oct-2008 13:54	1.4M	
tor-im-browser-1.1.4_en-US_split.part06.rar	13-Oct-2008 13:54	1.4M	
tor-im-browser-1.1.4_en-US_split.part07.rar	13-Oct-2008 13:54	1.4M	

If the torproject.org Web site is filtered from where you are, type "tor mirrors" in your favorite Web search engine: the results probably include some alternative addresses to download the Tor Browser Bundle.

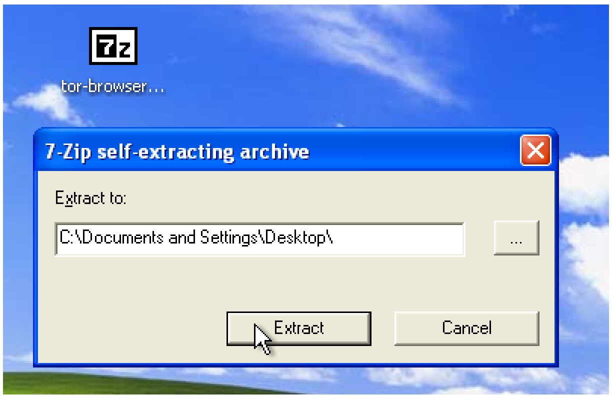
Caution: When you download Tor Bundle (plain or split versions), you should check the signatures of the files, especially if you are downloading the files from a mirror site. This step ensures that the files have not been tampered with. To learn more about signature files and how to check them, read https://wiki.torproject.org/noreply/TheOnionRouter/VerifyingSignatures

(You can also download the GnuPG software that you will need to check the signature here: http://www.gnupg.org/download/index.en.html#auto-ref-2).

Auto-extract the archive

- To get started, double-click the .EXE file you just downloaded.

  You should see the window below:

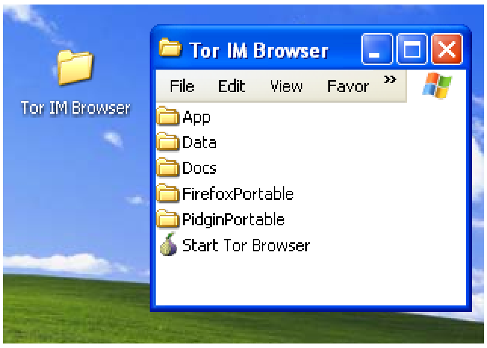


Extract to: C:\Documents and Settings\Desktop\

- Choose a folder into which you want to extract the files. If you are not sure leave the default value untouched. Then click "Extract".

  > **Note**: You can choose to extract the files directly onto a USB key or memory stick if you want to use Tor Browser on different computers (for instance on public computers in Internet cafÃ©s).

- When the extraction is completed, open the newly-created folder and check that it looks like the image below (note the "PidginPortable" folder):



- You can now safely delete the ".exe" file you originally downloaded (or the several ".rar" and ".exe" files if you used the split version).

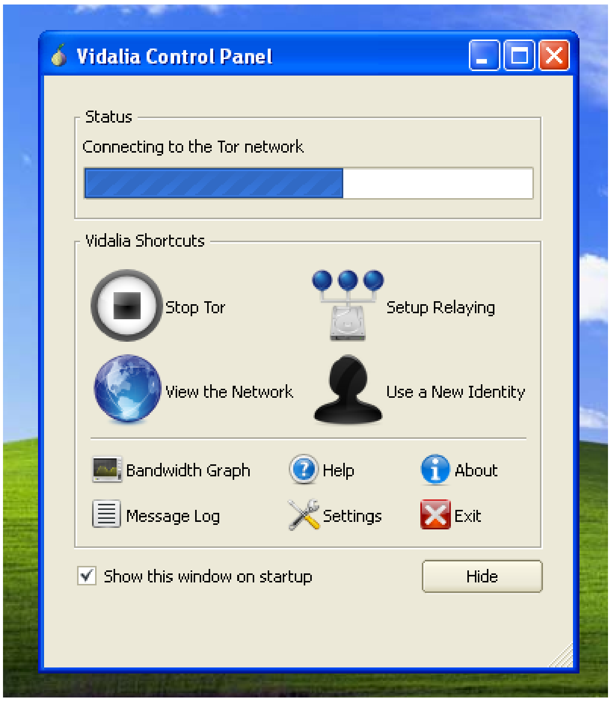
Using Tor IM Browser Bundle

Before you start:

- **Close Firefox.** If the Firefox browser is installed on your computer, make sure it is not currently running.
- **Close Tor.** If Tor is already installed on your computer, make sure it is not currently running.

Launch Tor IM Browser:

- In the "Tor Browser" folder, double-click "**Start Tor Browser**". The Tor control panel ("Vidalia") opens and Tor connects to the Tor network.

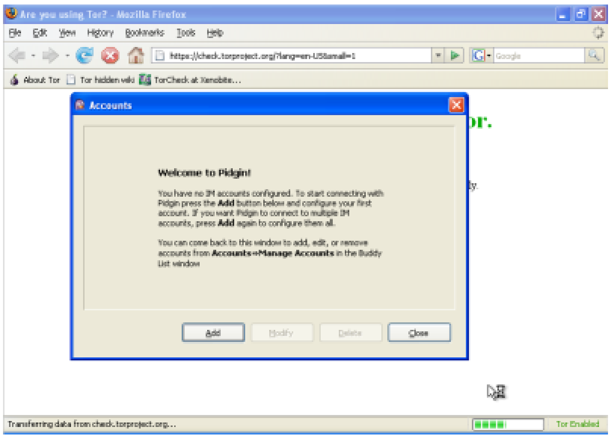


Connecting to the Tor network

☑ Show this window on startup

When a connection is established:

- A **Firefox browser window** pops up and connects to the TorCheck page, which should show a green onion that confirms you that you are connected to the Tor network.
- A **Pidgin assistant window** (below) pops up inviting you to set up your IM account on Pidgin.

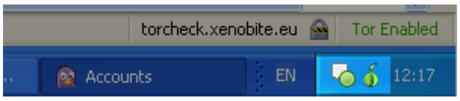

Are you using Tor? - Mozilla Firefox
File Edit View History Bookmarks Tools Help
https://check.torproject.org/?lang=en-US&small=1
About Tor
Tor hidden wiki
TorCheck at Xenobite...
Accounts
Add
Modify
Delete
Close
Transferring data from check.torproject.org...
Tor Enabled

Welcome to Pidgin!

You have no IM accounts configured. To start connecting with Pidgin press the **Add** button below and configure your first account. If you want Pidgin to connect to multiple IM accounts, press **Add** again to configure them all.

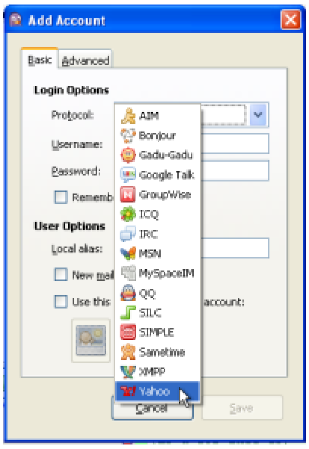
You can come back to this window to add, edit, or remove accounts from **Accounts→Manage Accounts** in the Buddy List window

You will also see the Tor icon (a green onion if you are connected) and a Pidgin icon appear in the System Tray on the lower-right-hand corner of your screen:



Set up your IM account in Pidgin

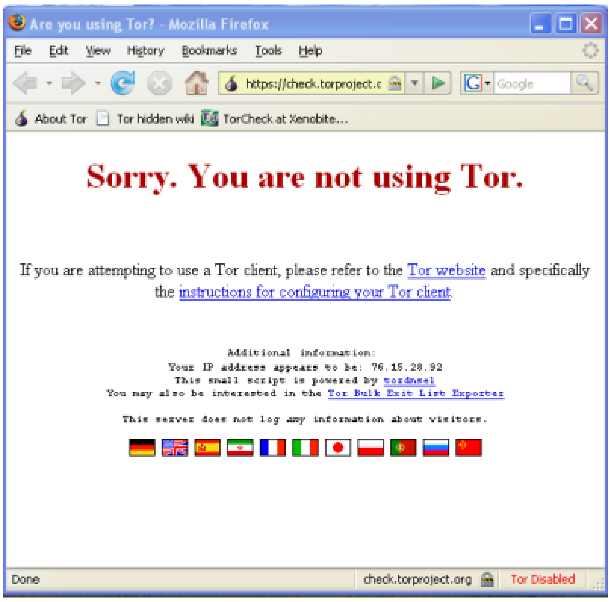
You can set up your IM account in the Pidgin window. Pidgin is compatible with most major IM services (AIM, MSN, Yahoo!, Google Talk, Jabber, XMPP, ICQ, and others):



To learn more on how you can use Pidgin, read:

http://developer.pidgin.im/wiki/Using%20Pidgin#GettingStarted

If this does not work



Sorry. You are not using Tor.

If you are attempting to use a Tor client, please refer to the Tor website and specifically the instructions for configuring your Tor client.

Additional information:
Your IP address appears to be: 76.15.28.92
This small script is powered by tordnsel
You may also be interested in the Tor Bulk Exit List Exporter

This server does not log any information about visitors.

If the onion in the Vidalia Control Panel doesn't turn green or if Firefox opens, but displays a page saying "Sorry. You are not using Tor", then you should:

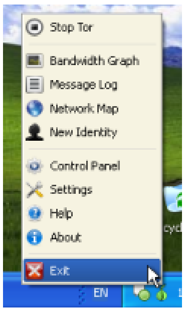
- **Exit Vidalia and Pidgin** (see below for details).
- **Relaunch Tor IM Browser** following the steps above ("Using Tor IM Browser Bundle").

If Tor Browser still doesn't work, after two or three tries, Tor may be partly blocked by your ISP. Refer to the "**Using Tor with Bridges**" chapter of this manual and try again, using the bridge feature of Tor.

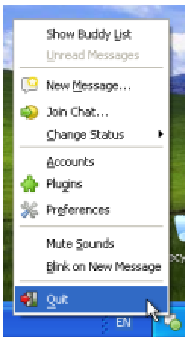
Exit Tor IM Browser

To exit the Tor IM Browser you need to:

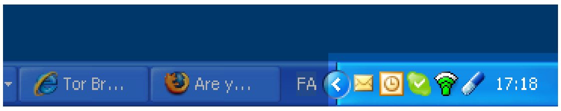
- **Exit Vidalia** by right-clicking on the onion icon in your tray bar and choose "Exit" in the Vidalia contextual menu.



- **Exit Pidgin** by right clicking on the Pidgin icon in your tray bar and choose "Quit" in the Pidgin contextual menu



When the Vidalia onion icon and the Pidgin icon have disappeared from the Windows System Tray in the lower-right-hand corner of your screen, Tor IM Browser is closed.



Using Tor with Bridges

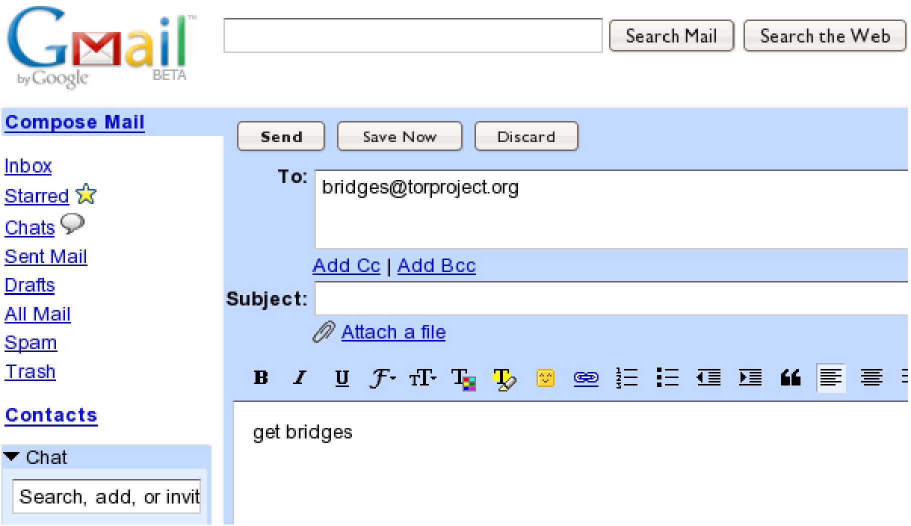
If you suspect your access to the Tor network is being blocked, you may want to use the bridge feature of Tor. The bridge feature was created specifically to help people use Tor from places where access to the Tor network is blocked. (You must already have successfully downloaded and installed the Tor software to use a bridge.)

What is a bridge?

Bridge relays (or "bridges" for short) are Tor relays that aren't listed in the main public Tor directory. This is a deliberate measure to stop these relays from being blocked. Even if your Internet service provider is filtering connections to all the publicly known Tor relays, it may not be able to block all the bridges.

Where do I find bridges?

To use a bridge, you need to locate one and add its information in your network settings. Send an e-mail from a **Gmail** account to **bridges@torproject.org** with the line "**get bridges**" -- by itself -- in the body of the mail.

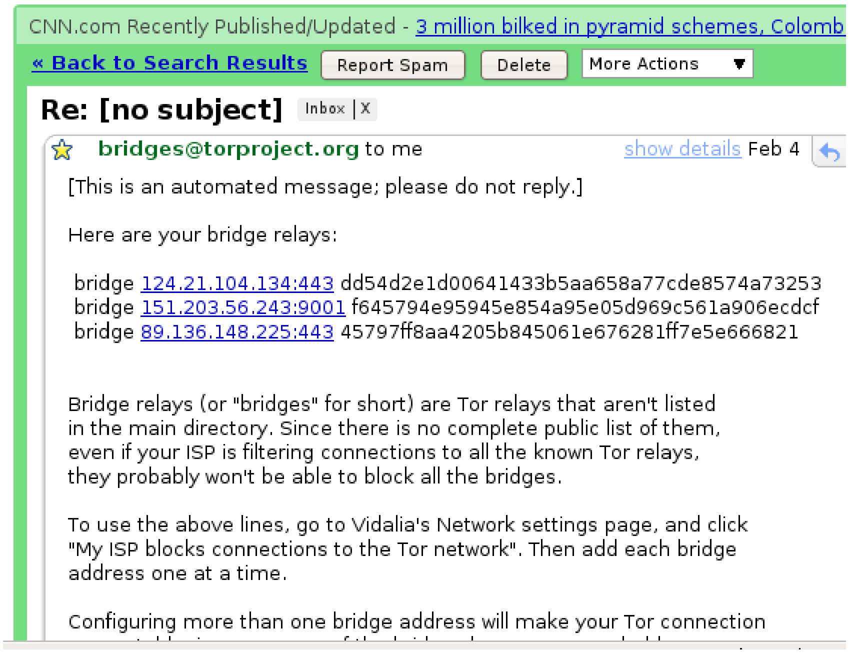


To: bridges@torproject.org

Subject:

get bridges

Almost instantly, you will receive a reply that includes information about a few bridges:



CNN.com Recently Published/Updated - 3 million bilked in pyramid schemes, Colomb

« Back to Search Results | Report Spam | Delete | More Actions ▼

Re: [no subject] Inbox | X

☆ bridges@torproject.org to me show details Feb 4

[This is an automated message; please do not reply.]

Here are your bridge relays:

```
 bridge 124.21.104.134:443 dd54d2e1d00641433b5aa658a77cde8574a73253
 bridge 151.203.56.243:9001 f645794e95945e854a95e05d969c561a906ecdcf
 bridge 89.136.148.225:443 45797ff8aa4205b845061e676281ff7e5e666821
```

Bridge relays (or "bridges" for short) are Tor relays that aren't listed in the main directory. Since there is no complete public list of them, even if your ISP is filtering connections to all the known Tor relays, they probably won't be able to block all the bridges.

To use the above lines, go to Vidalia's Network settings page, and click "My ISP blocks connections to the Tor network". Then add each bridge address one at a time.

Configuring more than one bridge address will make your Tor connection

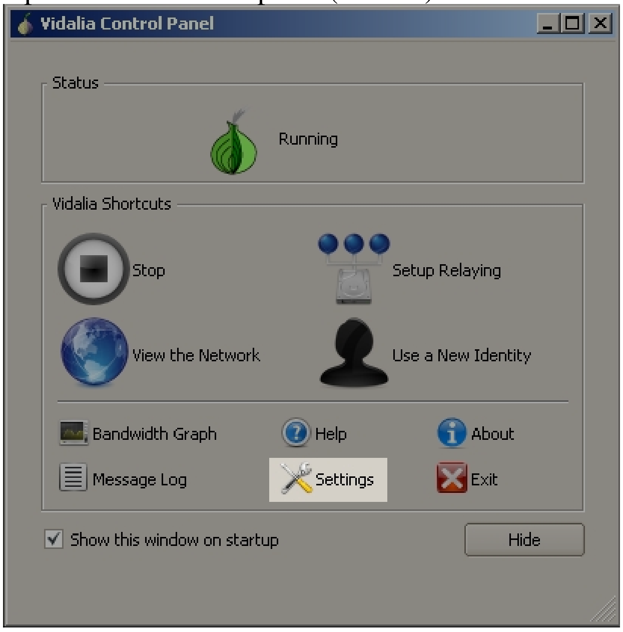
Important Notes:

1. You *must* use a Gmail account to send the request. If torproject.org accepted requests from other mail accounts, an attacker could easily create a lot of email addresses and quickly learn about all the bridges. If you do not have a Gmail account already, creating one takes only a few minutes.
2. It is generally recommended to use Gmail with a secure SSL connection at "https://mail.google.com", rather than the unencrypted URL "http://mail.google.com/". On the Gmail settings page you can make HTTPS the default, in case you forget to use the https: prefix.
3. If you are on a slow Internet connection you can use the URL https://mail.google.com/mail/h/ for a direct access to the basic HTML version of Gmail.

Turn on bridging and enter bridge information

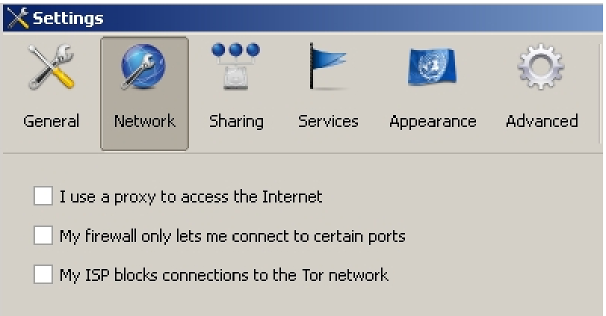
After you get addresses for some bridge relays, you must configure Tor with whatever bridge address you intend to use:

1. Open the Tor control panel (Vidalia).



☑ Show this window on startup

2. Click "Settings". A "Settings" window opens.

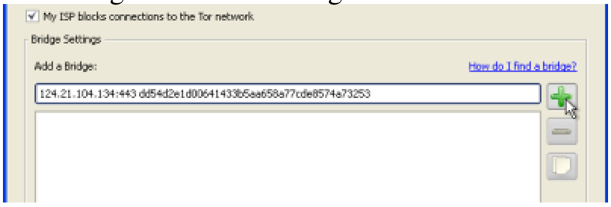


□ I use a proxy to access the Internet

□ My firewall only lets me connect to certain ports

□ My ISP blocks connections to the Tor network

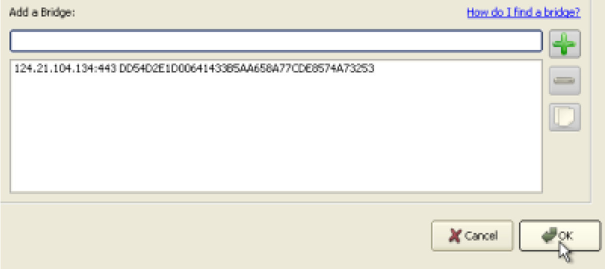
3. Click "Network".
4. Select "My Firewall only lets me connect to certain ports" and "My ISP blocks Connections to the Tor network".
5. Enter the bridge URL information you received by e-mail in the "Add a Bridge" field.
6. Click the green "+" on the right side of the "Add a Bridge" field. The URL is added to the box below.



☑ My ISP blocks connections to the Tor network

Add a Bridge: 124.21.104.134:443 dd54d2e1d00641433b5aa658a77cde8574a73253

7. Click "OK" at the bottom of the window to validate your new settings.



Add a Bridge:

124.21.104.134:443 DD54D2E1D00641433B5AA658A77CDE8574A73253

8. In the Tor control panel, stop and restart Tor to use your new settings.

Note:

Add as many bridge addresses as you can. Additional bridges increase reliability. One bridge is enough to reach the Tor network, however, if you have only one bridge and it gets blocked or stops operating, you will be cut off from the Tor network until you add new bridges.

To add more bridges in your network settings, repeat the steps above with the information on the additional bridges that you got from the bridges@torproject.org e-mail message.

About JonDo

JonDo is a proxy tool similar to Tor which can be used to bypass Internet censorship. It was invented in 2000 as a German university project called Java Anon Proxy (JAP) and now offers both free and commercial services. The free servers only offer the speed of an analog modem whereas the commercial service offers higher speed for about 10 US Dollars for 1 GB of traffic. The Java client runs on Linux, Mac OS and Windows.

Like Tor, JonDo's main purpose is to provide anonymity for users when visiting Web sites. Like Tor, it works by sending traffic through several independent servers.

Installation

To use the JonDo network you need to download the JonDo client for your operating system from https://www.jondos.de/en/download. For either Linux and Mac OS X there is a single download option (6 MB).

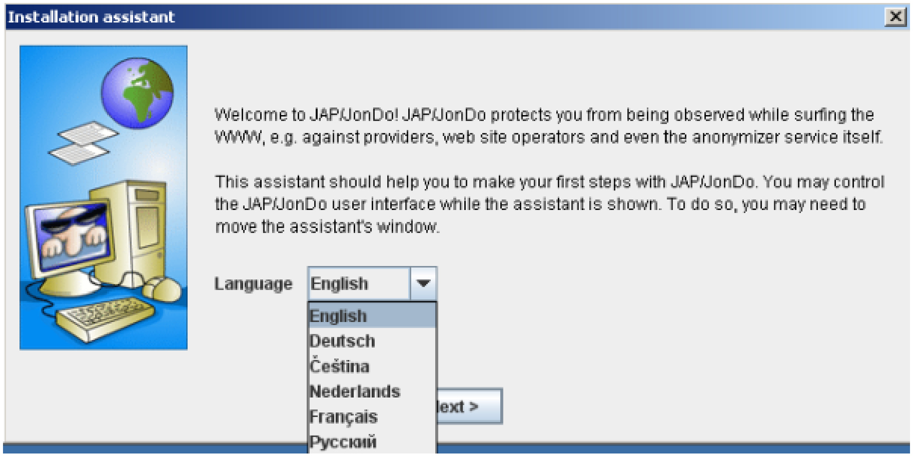
For Windows however, there are three different possibilities:

- The standard desktop installer which has Java included (about 15MB)
- A PortableApps version also with Java included which can be run from a USB flash drive for use at Internet cafÃ©s or other shared computers (about 20MB)
- The minimal three-file download necessary to run JonDo without the installer and Java: It consists of the files http://anon.inf.tu-dresden.de/develop/jap.exe, http://anon.inf.tu-dresden.de/develop/japdll.dll and http://anon.inf.tu-dresden.de/jap/JAP.jar (in total about 6MB).

Choose a download depending on your experience, intended use and speed of your Internet connection. To install the JonDo client you just have to click on the downloaded file and follow the simple instructions.

Configuration and Usage

When you first start JonDo you see a window where you can choose between the languages English, German, Czech, Dutch, French and Russian.



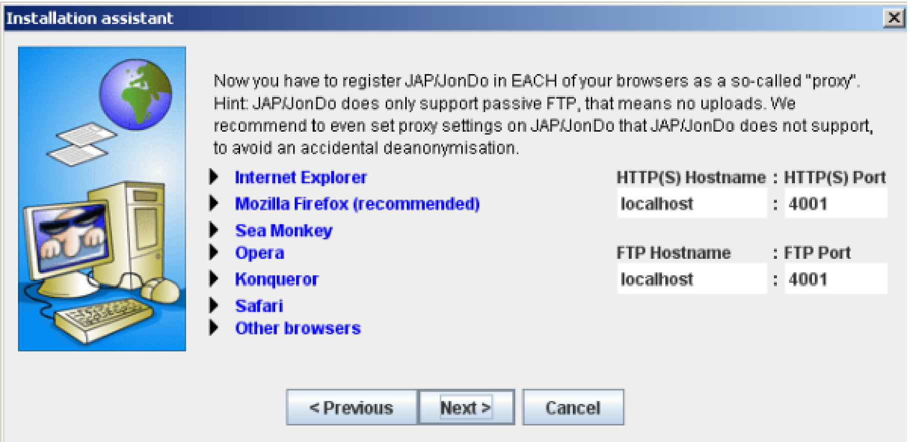
Installation assistant

Welcome to JAP/JonDo! JAP/JonDo protects you from being observed while surfing the WWW, e.g. against providers, web site operators and even the anonymizer service itself.

This assistant should help you to make your first steps with JAP/JonDo. You may control the JAP/JonDo user interface while the assistant is shown. To do so, you may need to move the assistant's window.

Language: English

On the next screen, you will see a notice that you have to configure your Web browser to use the JonDo proxy tool. Click on the name of your browser and follow the instructions you get.



Installation assistant

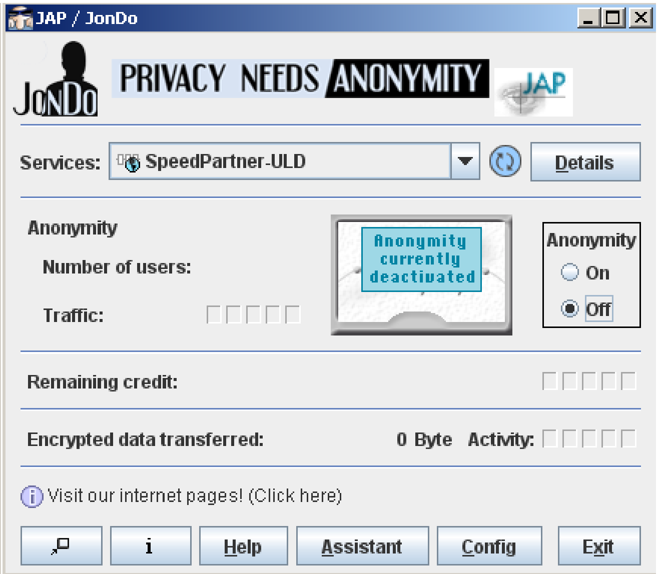
Now you have to register JAP/JonDo in EACH of your browsers as a so-called "proxy". Hint: JAP/JonDo does only support passive FTP, that means no uploads. We recommend to even set proxy settings on JAP/JonDo that JAP/JonDo does not support, to avoid an accidental deanonymisation.

- Internet Explorer
- Mozilla Firefox (recommended)
- Sea Monkey
- Opera
- Konqueror
- Safari
- Other browsers

HTTP(S) Hostname	:	HTTP(S) Port
localhost	:	4001

FTP Hostname	:	FTP Port
localhost	:	4001

Now take the first step to check if you configured your browser correctly. Switch anonymity to "Off" in the JonDo main window and then open a Web site with the browser you just configured.



JAP / JonDo

Services: SpeedPartner-ULD

Anonymity

Number of users:

Traffic:

Anonymity currently deactivated

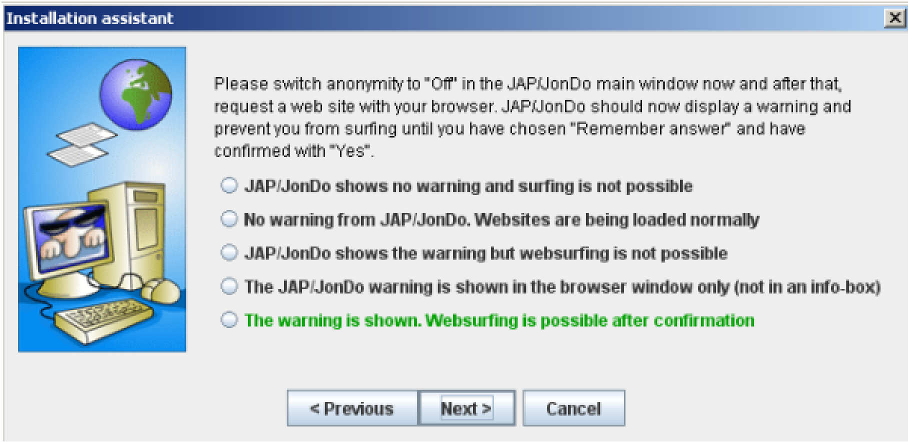
Anonymity
○ On
● Off

Remaining credit:

Encrypted data transferred: 0 Byte Activity:

Visit our internet pages! (Click here)

If JonDo shows you a warning and you have to choose "Yes" to view the Web site everything is configured properly and you can choose "*The warning is shown. Websurfing is possible after confirmation*". If any other description applies to you, choose it and the Installation assistant will give you more information on how to solve the problem.

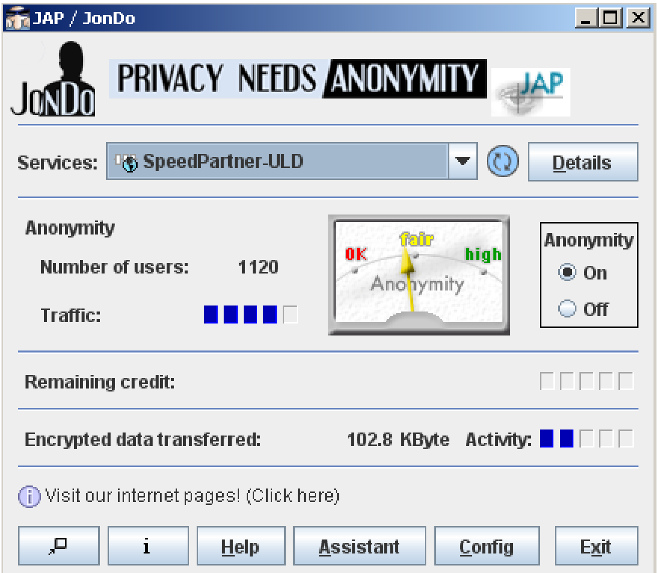


Installation assistant

Please switch anonymity to "Off" in the JAP/JonDo main window now and after that, request a web site with your browser. JAP/JonDo should now display a warning and prevent you from surfing until you have chosen "Remember answer" and have confirmed with "Yes".

○ JAP/JonDo shows no warning and surfing is not possible
○ No warning from JAP/JonDo. Websites are being loaded normally
○ JAP/JonDo shows the warning but websurfing is not possible
○ The JAP/JonDo warning is shown in the browser window only (not in an info-box)
○ The warning is shown. Websurfing is possible after confirmation

Now take the second step to ensure a proper configuration: switch anonymity to "On" in the main JonDo window and again open a random Web site with the browser you configured.



Services: SpeedPartner-ULD

Anonymity

Number of users: 1120

Traffic: ■■■■□

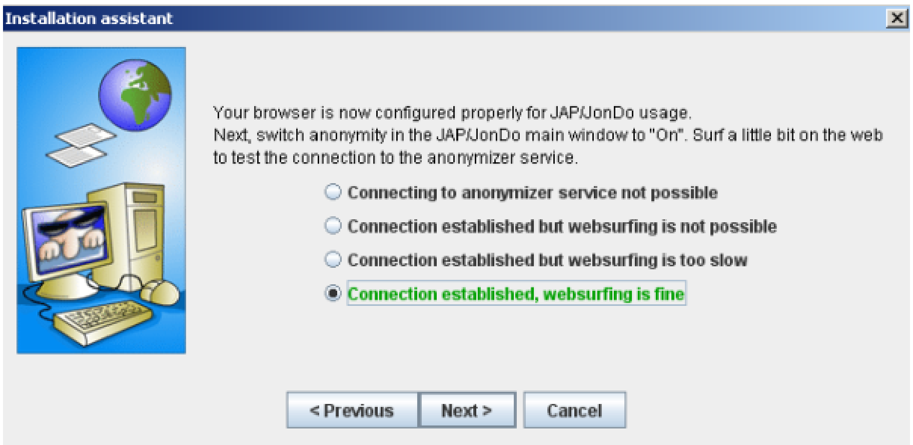
Anonymity
● On
○ Off

Remaining credit: □□□□□

Encrypted data transferred: 102.8 KByte Activity: ■■□□□

Visit our internet pages! (Click here)

If the Web site loads, everything is fine and you can click "*Connection established, websurfing is fine*". If another description applies to you choose that one and the Installation assistant will help you solve the problem.

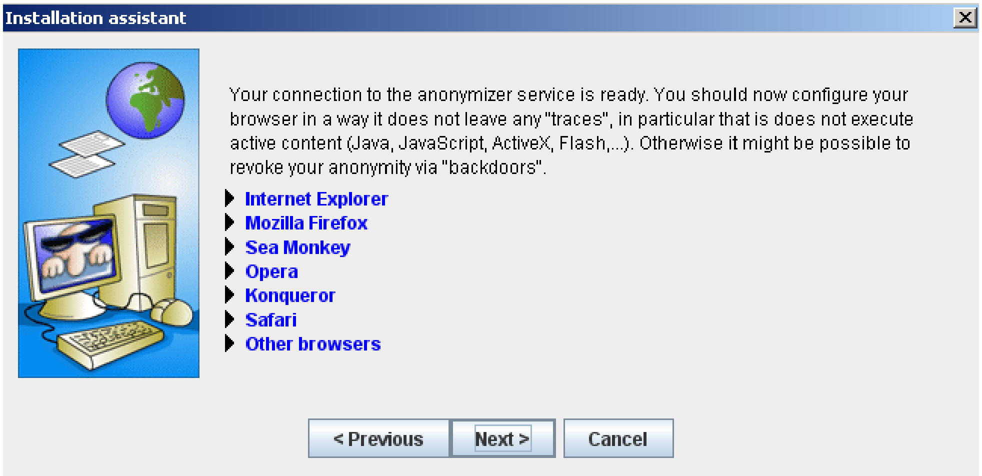


Installation assistant

Your browser is now configured properly for JAP/JonDo usage.
Next, switch anonymity in the JAP/JonDo main window to "On". Surf a little bit on the web to test the connection to the anonymizer service.

○ Connecting to anonymizer service not possible
○ Connection established but websurfing is not possible
○ Connection established but websurfing is too slow
● Connection established, websurfing is fine

Now the configuration is almost done. You are already browsing through the JonDo network. However, you should configure your Web browser so that it doesn't leak any information. This again is explained when you click on the name of your Web browser.



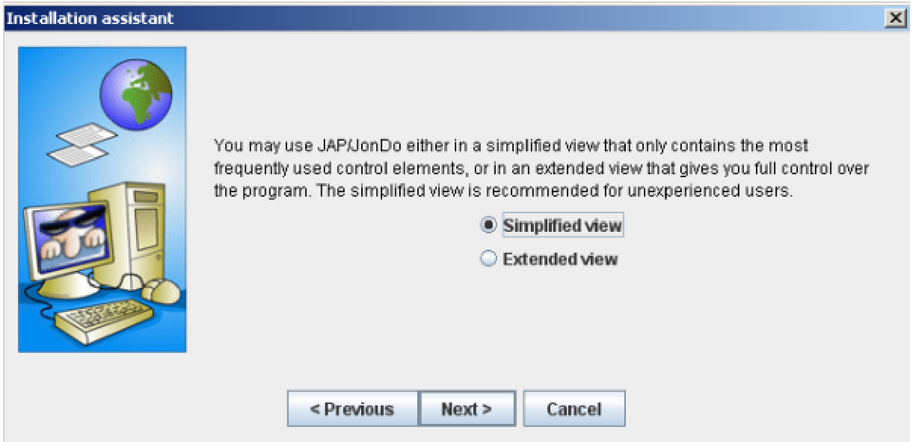
Installation assistant

Your connection to the anonymizer service is ready. You should now configure your browser in a way it does not leave any "traces", in particular that is does not execute active content (Java, JavaScript, ActiveX, Flash,...). Otherwise it might be possible to revoke your anonymity via "backdoors".

- Internet Explorer
- Mozilla Firefox
- Sea Monkey
- Opera
- Konqueror
- Safari
- Other browsers

Now choose the options you want to see in the JonDo client based on your computer experience.

Inexperienced users should choose "Simplified view".

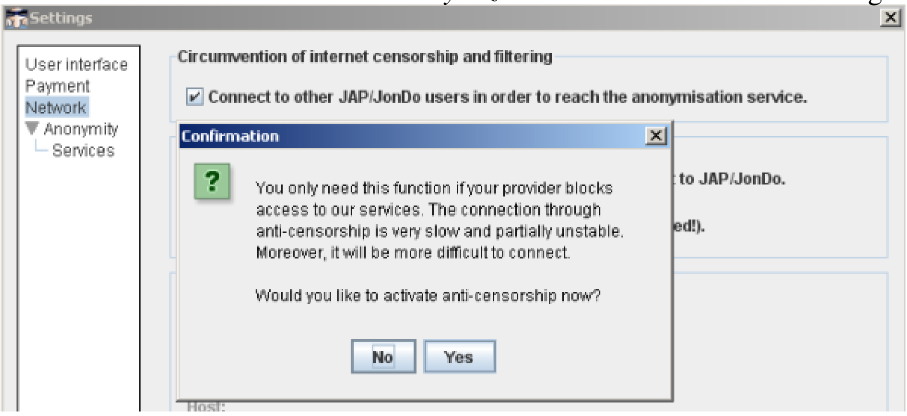


You may use JAP/JonDo either in a simplified view that only contains the most frequently used control elements, or in an extended view that gives you full control over the program. The simplified view is recommended for unexperienced users.

● Simplified view

○ Extended view

If the standard JonDo servers are already blocked in your country, you should try the anti-censorship option. Click on "*Config*" in the main JonDo window and select the "*network*" tab. There click on "Connect to other JAP/JonDo users *in order to reach the anonymization service*". Read the warning and confirm it by clicking "*Yes*".



Circumvention of internet censorship and filtering

☑ Connect to other JAP/JonDo users in order to reach the anonymisation service.

You only need this function if your provider blocks access to our services. The connection through anti-censorship is very slow and partially unstable. Moreover, it will be more difficult to connect.

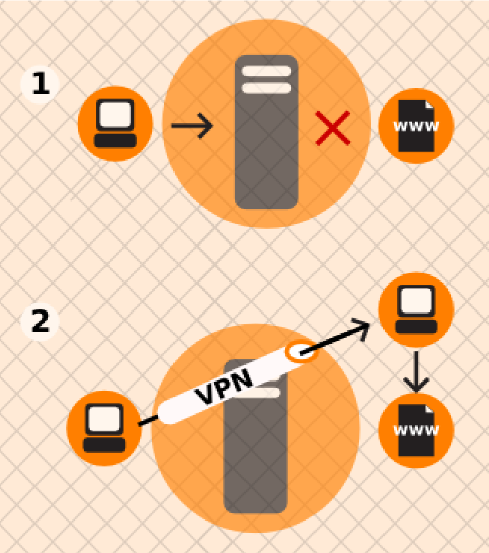
Would you like to activate anti-censorship now?

What are VPN and Tunneling?

VPN (virtual private network) and **tunneling** are techniques that allow you to encrypt the data connections between yourself and another computer. This computer might belong to your organization, a trusted contact or a commercial VPN service. Tunneling encapsulates a specific stream of data within an encrypted protocol, making everything that travels through the tunnel unreadable to anyone along the way. VPNs are very commonly used by corporations to allow employees who need access to sensitive financial or other information to access the companies' computer systems from home or other remote locations over the Internet.

Using a VPN or other kinds of tunnels to encrypt your information can be a good way of ensuring it is not seen by anyone but yourself and people you trust. It has the additional effect of making all your different kinds of traffic look similar to an eavesdropper or to a system that is trying to block your traffic. Since many international companies use VPN technology, it is not very likely to be blocked.

These techniques create a tunnel from your computer to another computer somewhere on the Internet. Your data can travel through this tunnel and then continue to a final destination on the Web. The integrity and privacy of the traffic inside the tunnel are protected by encryption.



If the tunnel ends outside the area where the Internet is being restricted, this can be an effective method of circumvention, since the filtering entity/server sees only encrypted data, and has no way of knowing what data is passing through the tunnel.

It is important to note that the data is only encrypted as far as the end of the tunnel, and then travels unencrypted to its final destination. If, for example, you set up a tunnel to a commercial VPN provider, and then request the Web page news.bbc.co.uk through the tunnel, the data will be encrypted from your computer to the VPN provider's computer at the other end, but from there it will be unencrypted to the servers run by the BBC, just like normal Internet traffic. This means that the VPN provider, the BBC and anyone with control over a system between these two servers, will, in theory, be able to see what data you have requested.

Tunneling

The main difference between a VPN connection and a tunnel is that a VPN system is set up in such a way that it encrypts all data from your computer to the Internet, while a **tunnel** is set up to encrypt only traffic from specific applications, either based on the **port numbers** they use or by requiring you to specify which tunnel to use within each application. Unlike a VPN, tunnels require each application, such as a Web browser, e-mail client or Instant Messaging program, that needs to use the encrypted tunnel, to be configured individually to use the tunnel. Significantly, not all applications are capable of being passed through common types of tunnels. Most Voice over IP (VoIP) systems, for example, use the **UDP** protocol, which is not supported in many common tunneling systems. Also, some common applications such as the Opera web browser do not have built-in support for **SOCKS proxies** which are the most common type of tunneling software. In this case you have to use an extra application like FreeCap for Windows (http://www.freecap.ru/eng/) or tsocks for Linux (http://tsocks.sourceforge.net/).

Once a tunnel is established and applications have been configured, they will run through the encrypted tunnel to the computer with the tunneling software, which forwards your requests and responses transparently. Users with contacts in a non-filtered country can set up private tunneling services while those without contacts can purchase commercial tunneling services, usually by monthly subscription for about 5 US Dollars a month (usually requiring a credit card payment).

Various free tunneling services are also available. When using free tunneling services users should note that they often include advertisements. Requests for the advertisements sometimes are conducted through unencrypted **plain text HTTP requests**, which can be intercepted by any intermediary who can then determine that the user is using a tunneling service. Moreover, many tunneling services rely on the use of SOCKS proxies which may leak **domain name** requests. Some commercially available tunneling systems which also provide a (slow) free service are:

- http://www.http-tunnel.com/
- http://www.hopster.com/
- http://www.htthost.com/

VPN

Unlike tunnels, VPN systems transport all data over the encrypted network, including **Voice over IP** (VoIP) and communications from applications with no built-in support for SOCKS. Once VPNs are set up, they are much more comprehensive tools than tunnels, but they are more complicated to set up and configure than most tunneling applications.

There are a number of different standards for setting up VPN networks, including **IPSec**, **SSL/TLS** and **PPTP**, that vary in terms of complexity, the level of security they provide, and which operating systems they are available for. Naturally, there are also many different implementations of each standard within software that have various other features.

- While PPTP is known to use weaker encryption than either IPSec or SSL/TLS, it may be useful for bypassing Internet blocking, and the client software is conveniently built into most versions of Microsoft Windows.
- SSL/TLS-based VPN systems are relatively simple to configure, and provide a solid level of security.
- IPSec runs at the Internet level, responsible for packet transfer, in the Internet architecture, while the others run at the Application level. This makes IPsec more flexible, as it can be used for protecting all the higher level protocols. Applications do not need to be designed to use IPsec, whereas SSL/TLS or other higher-layer protocol functions must be built into an application.

VPNs are frequently used by companies and organizations as private communication channels to connect securely over the Internet. Because of their popularity there are many commercial providers of VPN services, which allow you to purchase access to a VPN service for a fee. Using such a service requires you to trust the owners of the service, but provides a simple and convenient method of bypassing Internet filtering for a monthly fee of about 5-10 US Dollars. There is a list of commercial VPN providers available at http://en.cship.org/wiki/VPN.

As an alternative to paying for commercial VPN services, users with contacts in unrestricted locations may have these contacts download and install software that sets up a private VPN service. This requires a much higher level of technical knowledge, but it will be free. Also the private nature of such a setup means it is less likely to be blocked than a commercial service that has been available for a long time. One of the most widely used free and open source programs available for setting up this kind of private VPN is OpenVPN (http://openvpn.net/), which can be installed on Linux, MacOS, Windows and many other operating systems.

Advantages

Tunneling applications and VPNs provide encrypted transfer of your data. They generally have the ability to securely proxy many different functions, not just web traffic. So it is one of the safest ways to bypass Internet censorship. Once configured it is also easy to use.

Tunneling applications and VPNs are best suited for technically capable users who require secure circumvention services for more than just web traffic and do access the Internet from their own computer where they can install additional software. Commercial tunneling services are an excellent resource for users in censored locations who do not have trusted contacts in non-filtered locations, VPN technology is a common business application that is not likely to be blocked.

Some, but not all, commercial tunnel and VPN services advertise anonymity, which privately set up services generally can't achieve. This anonymity protection can be fairly effective if the commercial VPN or tunnel operator is trustworthy.

Disadvantages and Risks

Commercial tunneling services and commercial VPNs are publicly known and may already be filtered. They normally cannot be used by users in public access locations where users cannot install software, such as Internet cafÃ©s or libraries. Use of tunneling applications and especially VPNs may require a higher level of technical expertise than other circumvention methods.

A network operator can detect that a VPN is being used and determine who the VPN provider is. The network operator should not be able to view the communications sent over the VPN unless the VPN is set up incorrectly.

The VPN or tunnel operator (much like a proxy operator) can see what you're doing unless you use some additional encryption for your communications; when you don't use additional encryption, you have to trust the VPN or tunnel operator not to abuse this access.

Using OpenVPN

OpenVPN is a well-respected, free open-source virtual private network (VPN) solution. It works on most versions of Windows (Windows Vista support is expected soon), Mac OS X and Linux. OpenVPN is **SSL**-based, which means it uses the same type of encryption that is used when visiting secure Web sites where the URL starts with http**s**.

OpenVPN is not suitable for temporary use in Internet cafÃ©s or elsewhere on shared computers where you can't install additional software.

In an OpenVPN system, there is one computer set up as a server (in an unrestricted location), and one or more clients. The server must be set up to be accessible from the Internet, not blocked by a **firewall** and with a **publicly routable IP address** (in some places, the person establishing the server may have to request this from her/his ISP). Each client connects to the server and creates a VPN "tunnel" through which traffic from the client can pass.

There are commercial OpenVPN providers such as WiTopia (http://witopia.net/personalmore.html) where you can purchase access to an OpenVPN server for a fee of about 5-10 US Dollar a month. These providers will also help you install and configure OpenVPN on your computer. A list of such commercial providers is available at http://en.cship.org/wiki/VPN.

OpenVPN also can be used by a trusted contact in an unfiltered location, providing an OpenVPN server to one or more clients and passing their traffic to his/her computer before continuing on to the Internet. Setting this up correctly is somewhat complicated, however.

Tips for setting up OpenVPN

To setup your own OpenVPN server and client follow the documentation provided by OpenVPN (http://openvpn.net/index.php/documentation/howto.html). If you want to use OpenVPN to visit blocked Web sites, the following notes are important:

Client

There is a **graphical user interface (GUI)** available for Windows which will make it easy to start and stop openVPN as required, and also enables you to configure OpenVPN to use an HTTP proxy to get onto the Internet. To download the GUI go to http://openvpn.se/.

To configure OpenVPN to use a proxy server in Linux or Mac OS X, read the relevant section on the Web site (http://openvpn.net/index.php/documentation/howto.html#http).

Server

- When choosing between routing and bridging, there is no additional advantage in configuring bridging when your clients just want to use it to bypass Internet censorship. Choose routing.
- Pay special attention to the section of the guide that explains how to ensure that all traffic from the client is passed through the server. Without this configuration the system will not help you visit blocked Web pages (http://openvpn.net/index.php/documentation/howto.html#redirect).
- If the client computer is behind a very restrictive firewall, and the default OpenVPN port is blocked, it is possible to change the port that OpenVPN uses. One option is to use port 443, which is normally used for secure websites (**HTTPS**), and to switch to **TCP** protocol instead of **UDP**. In this configuration, it is difficult for the firewall operators to tell the difference between OpenVPN traffic and normal secure Web traffic. To do this, near the top of the configuration files on both the client and server, replace "proto udp" with "proto tcp" and "port 1194" with "port 443".

Advantages and Risks

Once it is set up and configured correctly, OpenVPN can provide an effective way to bypass Internet filters. Since all traffic is encrypted between the client and the server, and can pass through a single port, it is very difficult to distinguish from any other secure Web traffic, such as data going to an online shopping site or other encrypted services.

OpenVPN can be used for all Internet traffic, including Web traffic, e-mail, instant messaging and Voice over IP.

OpenVPN also provides a degree of protection against surveillance, as long as you can trust the owner of the OpenVPN server, and you have followed the instructions in the OpenVPN documentation on how to handle the certificates and keys used. Remember that traffic is only encrypted as far as the OpenVPN server, after which it passes unencrypted onto the Internet.

The primary disadvantage of OpenVPN is the difficulty of installation and configuration. It also requires access to a server in an unrestricted location. OpenVPN also does not reliably provide anonymity.

SSH Tunnelling

SSH, the Secure Shell, is a standard protocol that encrypts communications between your computer and a server. The encryption prevents these communications from being viewed or modified by network operators. SSH can be used for a wide variety of secure communications applications, where secure log-in to a server and secure file transfers (**SCP** or **SFTP**) are the most common.

SSH is especially useful for censorship circumvention because it can provide encrypted tunnels and work as a generic proxy client. Censors may be reluctant to block SSH entirely because it is used for many purposes other than circumventing censorship; for example, it is used by system administrators to administer their servers over the Internet.

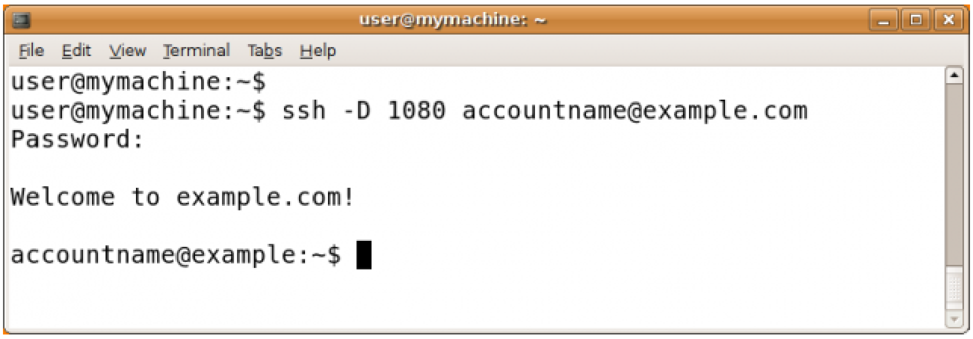
Using SSH requires an account on a server machine, generally a Unix or Linux server. For censorship circumvention, this server needs to have unrestricted Internet access and, ideally, is operated by a trusted contact. Some companies also sell accounts on their servers, and many Web hosting plans provide SSH access. You can find a list of shell account providers at http://www.google.com/Top/Computers/Internet/Access_Providers/Unix_Shell_Providers/ which sell accounts for about 2-10 US Dollars a month.

An SSH program called OpenSSH is already installed on most Unix, Linux, and Mac OS computers as a command-line program run from a terminal as "ssh." For Windows, you can also get a free SSH implementation called PuTTY.

All recent versions of SSH support creating a SOCKS proxy that can let a Web browser and a wide variety of other software use the encrypted SSH connection to communicate with the unfiltered Internet. In this example, we will describe only this use of SSH. The steps below will set up a SOCKS proxy on local port 1080 of your computer using a shell account called "accountname@example.com".

Linux/Unix and MacOS command-line (with OpenSSH)

OpenSSH is available from http://www.openssh.com/, but it comes pre-installed on Linux/Unix and Mac OS computers. You will need a shell account on a server with an unrestricted Internet connection.



```
user@mymachine:~$
user@mymachine:~$ ssh -D 1080 accountname@example.com
Password:

Welcome to example.com!

accountname@example:~$ █
```

The ssh command you'll run contains a local port number (typically 1080), a server name, and a username (account name). It looks like this:

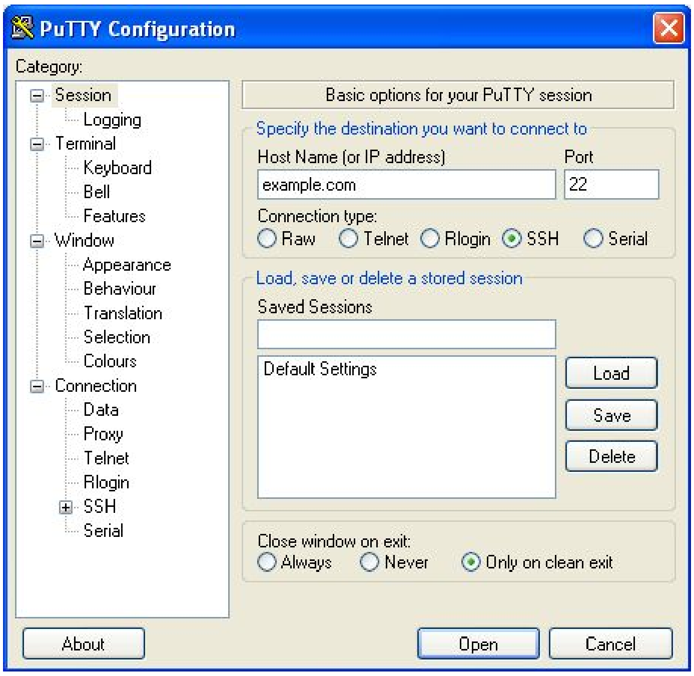
```
ssh -D localportnumber accountname@servername
```

You'll be prompted for your password and then you'll be logged into the server. With the use of the -D option, a local SOCKS proxy will be created and will exist as long as you're connected to the server. You can now proceed to verifying the host key and configuring your applications.

Windows graphical user interface (with PuTTY)

PuTTY is available from http://www.chiark.greenend.org.uk/~sgtatham/putty/download.html. You can save the putty.exe program on your hard drive for future use, or run it directly from the Web site (often, this is possible on a shared or public-access computer, such as a computer in a library or Internet cafÃ©).

When you start PuTTY, a session configuration dialog appears. You first enter the host name (address) of the SSH server you are going to connect to (here, "example.com"). If you only know the IP address or if DNS blocking is preventing you from using the host name, you can use the IP address instead. If you will perform these steps frequently, you can optionally create a PuTTY profile that saves these options as well as the options described below so they will be used every time.



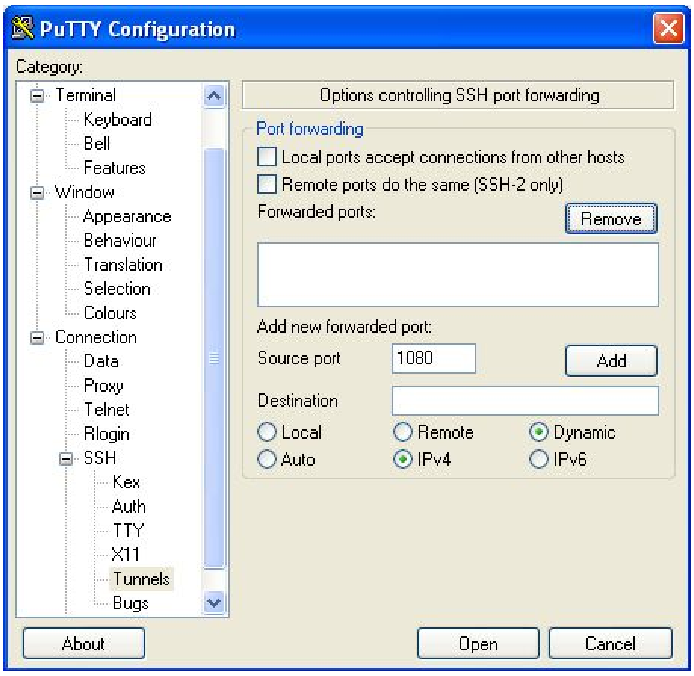
Host Name (or IP address): example.com
Port: 22

Connection type: ○ Raw ○ Telnet ○ Rlogin ● SSH ○ Serial

Close window on exit: ○ Always ○ Never ● Only on clean exit

Next, in the Category list, select Connection, then SSH, then Tunnels.

Enter 1080 for the Source port, and check the "Dynamic" and "IPv4" boxes.



Options controlling SSH port forwarding

Port forwarding

□ Local ports accept connections from other hosts

□ Remote ports do the same (SSH-2 only)

Forwarded ports:

Add new forwarded port:

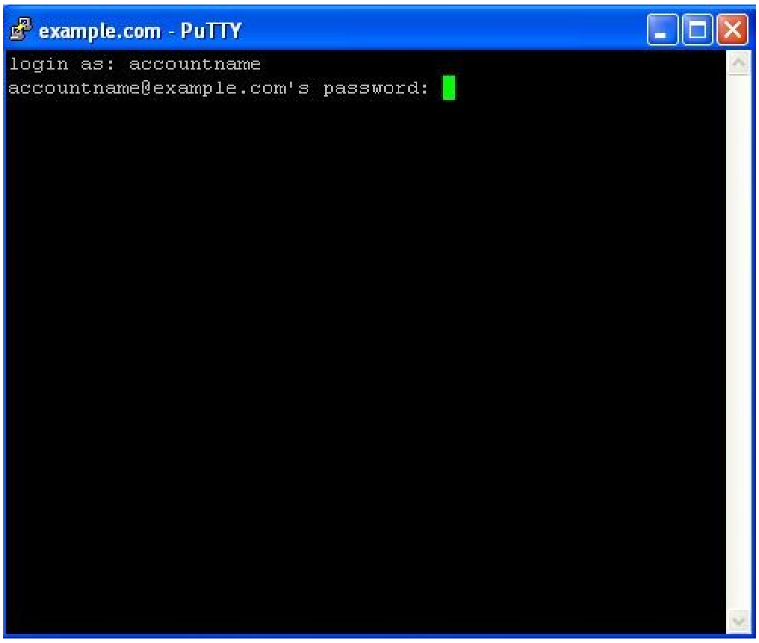
Source port 1080

Destination

○ Local ○ Remote ● Dynamic

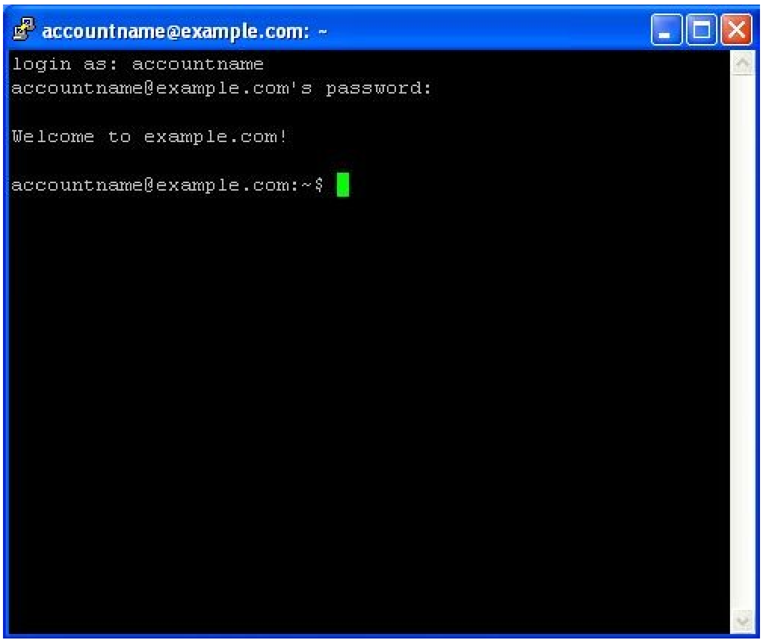
○ Auto ● IPv4 ○ IPv6

Now click the Add button, then the "Open" button. A connection is established to the server, and a new window is opened prompting for your username and password.



```
login as: accountname
accountname@example.com's password:
```

Enter this information and you will be logged into the server and receive a command line prompt from the server. The SOCKS proxy is then established.



```
login as: accountname
accountname@example.com's password:

Welcome to example.com!

accountname@example.com:~$
```

Host key verification

The first time you connect to a server, you should be prompted to confirm the **host key fingerprint** for that server. The host key fingerprint is a long sequence of letters and numbers (hexadecimal) like 57:ff:c9:60:10:17:67:bc:5c:00:85:37:20:95:36:dd that securely identifies a particular server.

Checking the host key fingerprint is a security measure to confirm that you are communicating with the server you think you are, and that the encrypted connection cannot be intercepted. (SSH does not provide a means of verifying this automatically. To get the benefit of this security mechanism, you should try to check the value of the host key fingerprint with the administrator of the server you're using, or ask a trusted contact to try connecting to the same server to see if they see the same fingerprint.)

Verifying host key fingerprints is important for ensuring that SSH protects the privacy of your communications against eavesdropping, but it isn't necessary if you only want to circumvent censorship and don't care if network operators can see the contents of your communications.

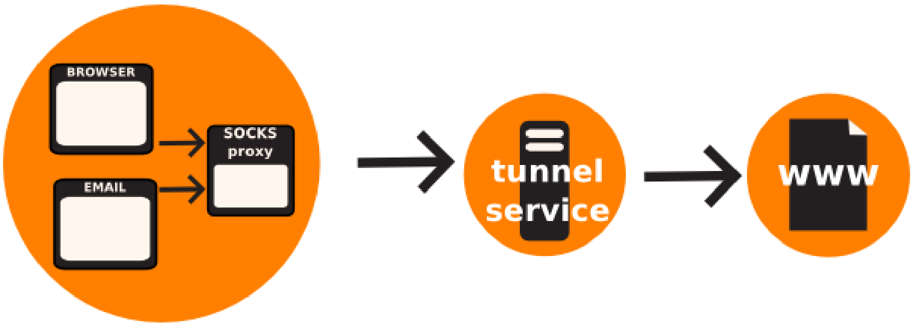
Configuring applications to use the proxy

The proxy created by the steps above should work until you close the SSH program. However, if your connection to the server is interrupted, you will need to repeat the same steps to reactivate the proxy.

Once the proxy is up and running, you need to configure software applications to use it. Using the steps above, the proxy will be a SOCKS proxy located on **localhost**, port 1080 (also known as 127.0.0.1, port 1080). You should try to ensure that your applications are configured in a way that prevents **DNS leaks**, which could make SSH less effective both for privacy protection and censorship circumvention.

Using Socks Proxies

A variety of software can take advantage of a SOCKS proxy to bypass filters or other restrictions â not only Web browsers, but also other Internet software like instant messaging and e-mail applications.



You can think of SOCKS proxies as a more advanced version of HTTP proxies, that allow many different kinds of Internet traffic from many different protocols to be sent through a tunnel, thereby bypassing blocks.

Although public SOCKS proxies do exist, in many cases SOCKS proxies will run locally on your computer, and will be provided by a software application. Because SOCKS tunnels are so flexible, some censorship circumvention software creates a **local proxy** running on your own computer (which is usually referred to by the name **localhost** or the IP address **127.0.0.1**). This local proxy is a way to let applications like a Web browser take advantage of the circumvention software. Tools that can work in this way include Tor, Your-Freedom and ssh tunnels set up with PuTTY.

Local proxy enthusiast T-shirt(get it?)

In order to use an application proxy for circumventing censorship, you must tell software on your computer that you want to use that proxy when communicating with other systems on the Internet.

Some Internet applications don't ordinarily work with a proxy because their developers didn't create them with proxy support. However, many of these applications can be made to work with a SOCKS proxy using "**socksifier**" software. Some examples of such software include:

- tsocks (http://tsocks.sourceforge.net/) on Unix/Linux
- WideCap (http://www.widecap.com/) on Windows
- ProxyCap (http://www.proxycap.com/) on Windows

Configuring Your Applications

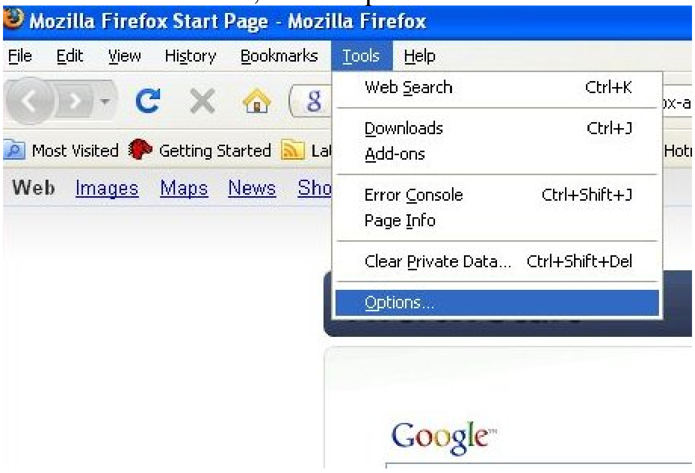
In most cases configuring applications to use a SOCKS proxy is done in much the same way as configuring them to use HTTP proxies. Applications that support SOCKS proxies will have a separate entry in the menu or configuration dialogue where HTTP proxies are configured which let you configure a SOCKS proxy. Some applications will ask you to choose between SOCKS 4 and SOCKS 5 proxy settings, and in most cases SOCKS 5 is the better option, although some SOCKS proxies may only work with SOCKS 4.

Some applications, such as Mozilla Firefox will allow you to configure both an HTTP proxy and a SOCKS proxy at the same time. In this case, normal web-browsing will happen through the HTTP proxy, and Firefox may use the SOCKS proxy for other traffic such as streaming video.

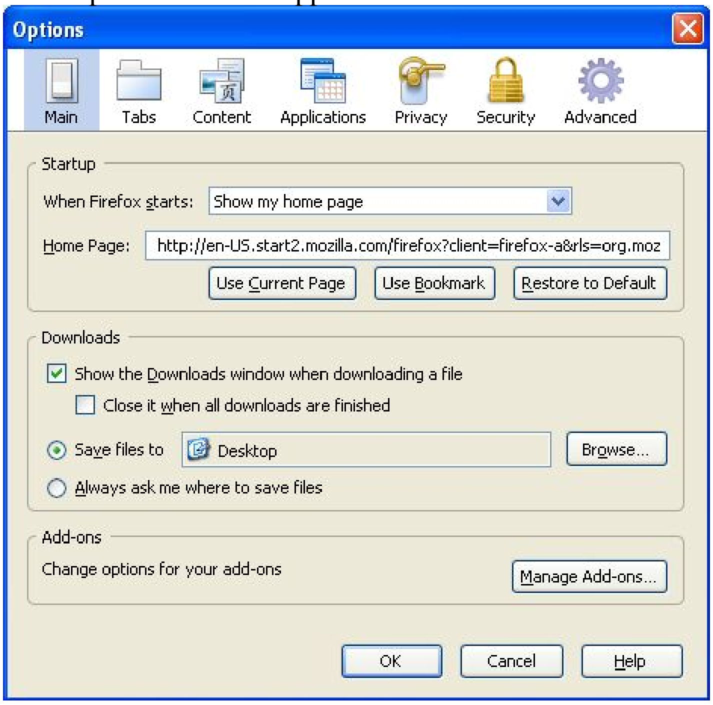
Mozilla Firefox

Enter settings as shown in the following image, and then click "OK".

1. On the "Tools" menu, click "Options":



2. The "Options" window appears:



When Firefox starts: Show my home page

Home Page: http://en-US.start2.mozilla.com/firefox?client=firefox-a&rls=org.moz

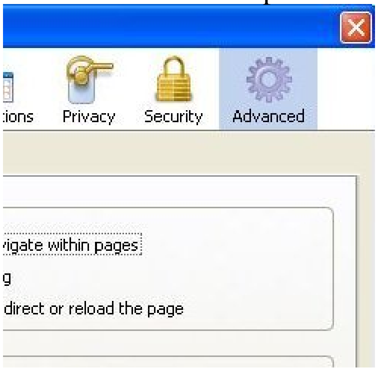
☑ Show the Downloads window when downloading a file

□ Close it when all downloads are finished

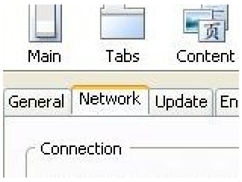
● Save files to: Desktop

○ Always ask me where to save files

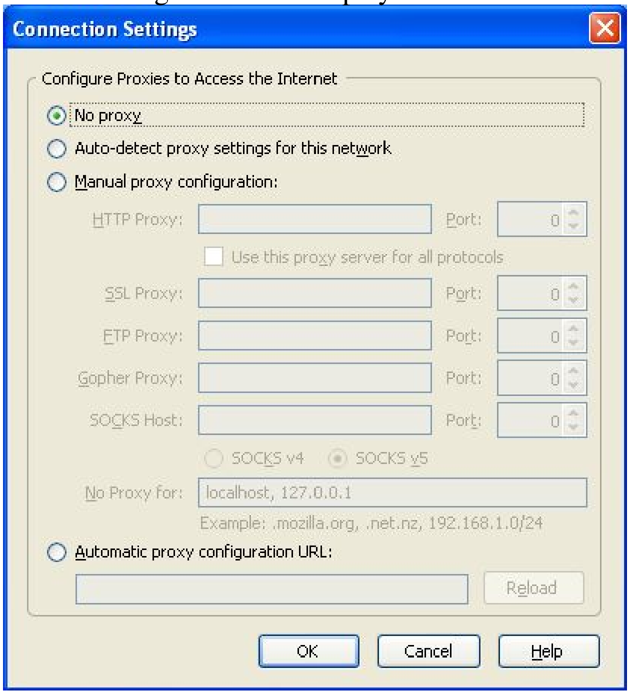
3. In the toolbar at the top of the window, click "Advanced":



4. Click the "Network" tab:



5. Click "Settings". Firefox displays the "Connection Settings" window:



Connection Settings

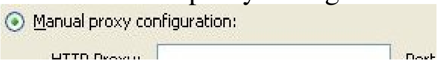
Configure Proxies to Access the Internet

● No proxy
○ Auto-detect proxy settings for this network
○ Manual proxy configuration:

HTTP Proxy: Port: 0
□ Use this proxy server for all protocols
SSL Proxy: Port: 0
FTP Proxy: Port: 0
Gopher Proxy: Port: 0
SOCKS Host: Port: 0
○ SOCKS v4 ● SOCKS v5
No Proxy for: localhost, 127.0.0.1
Example: .mozilla.org, .net.nz, 192.168.1.0/24

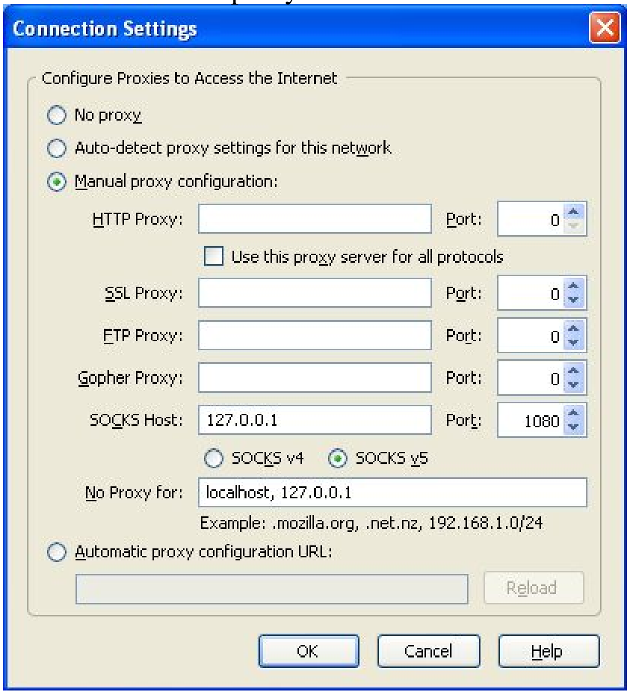
○ Automatic proxy configuration URL:

6. Select "Manual proxy configuration". The fields below that option become available.



● Manual proxy configuration:

7. Enter the "SOCKS proxy" address and "Port" number, choose "SOCKS v5" and then click "OK".



Connection Settings

Configure Proxies to Access the Internet

○ No proxy
○ Auto-detect proxy settings for this network
● Manual proxy configuration:

HTTP Proxy: Port: 0
□ Use this proxy server for all protocols
SSL Proxy: Port: 0
FTP Proxy: Port: 0
Gopher Proxy: Port: 0
SOCKS Host: 127.0.0.1 Port: 1080
○ SOCKS v4 ● SOCKS v5
No Proxy for: localhost, 127.0.0.1
Example: .mozilla.org, .net.nz, 192.168.1.0/24

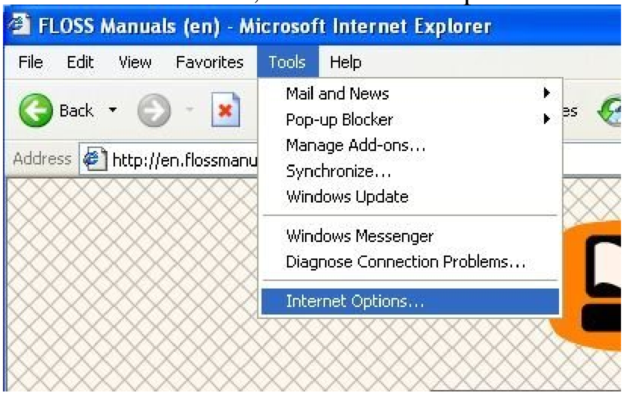
○ Automatic proxy configuration URL:

Now Firefox is configured to use a SOCKS proxy.

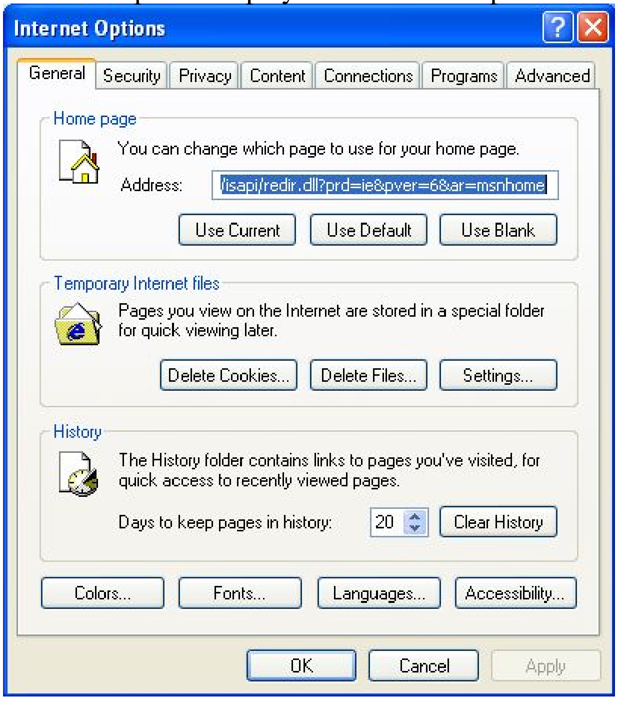
Microsoft Internet Explorer

To set Internet Explorer to use a SOCKS proxy:

1. On the "Tools" menu, click "Internet Options":



2. Internet Explorer displays the "Internet Options" window:



You can change which page to use for your home page.

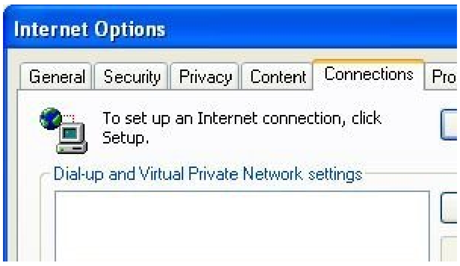
Address: /isapi/redir.dll?prd=ie&pver=6&ar=msnhome

Pages you view on the Internet are stored in a special folder for quick viewing later.

The History folder contains links to pages you've visited, for quick access to recently viewed pages.

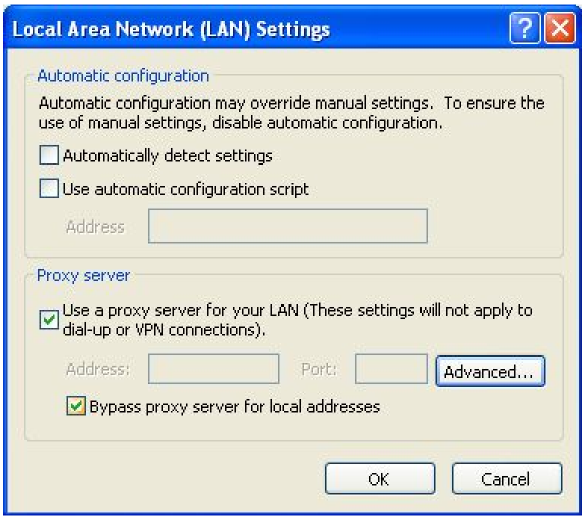
Days to keep pages in history: 20

3. Click the "Connections" tab:



To set up an Internet connection, click Setup.

4. Click "LAN Settings". Internet Explorer displays the "Local Area Network (LAN) Settings" window:


Local Area Network (LAN) Settings

Automatic configuration

Automatic configuration may override manual settings. To ensure the use of manual settings, disable automatic configuration.

□ Automatically detect settings

□ Use automatic configuration script

Address:

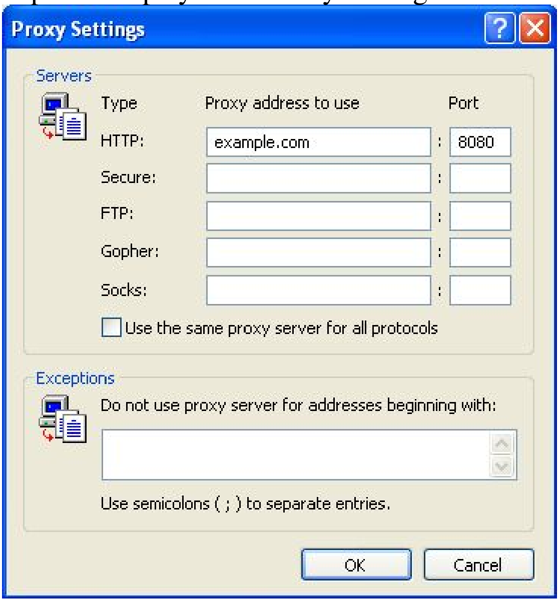
Proxy server

☑ Use a proxy server for your LAN (These settings will not apply to dial-up or VPN connections).

Address: Port:

☑ Bypass proxy server for local addresses

5. Select "Use a proxy server for your LAN" and click "Advanced". Internet Explorer displays the "Proxy Settings" window:


Proxy Settings

Servers

Type	Proxy address to use	Port
HTTP:	example.com	8080
Secure:		
FTP:		
Gopher:		
Socks:		

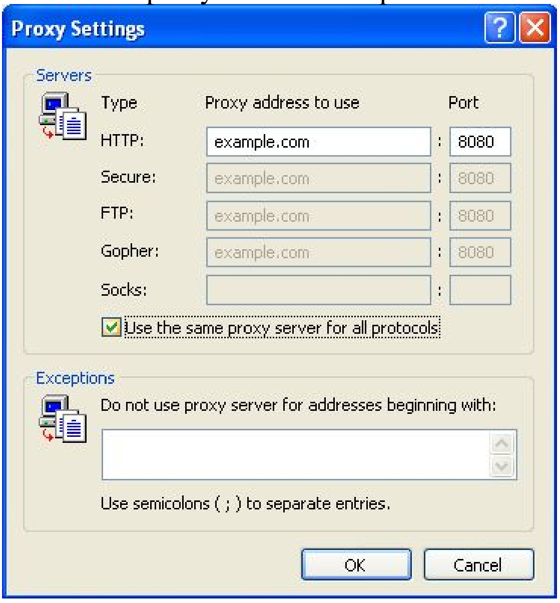
□ Use the same proxy server for all protocols

Exceptions

Do not use proxy server for addresses beginning with:

Use semicolons (;) to separate entries.

6. Clear "Use the same proxy server for all protocols" if it is selected:


Proxy Settings

Servers

Type	Proxy address to use	Port
HTTP:	example.com	8080
Secure:	example.com	8080
FTP:	example.com	8080
Gopher:	example.com	8080
Socks:		

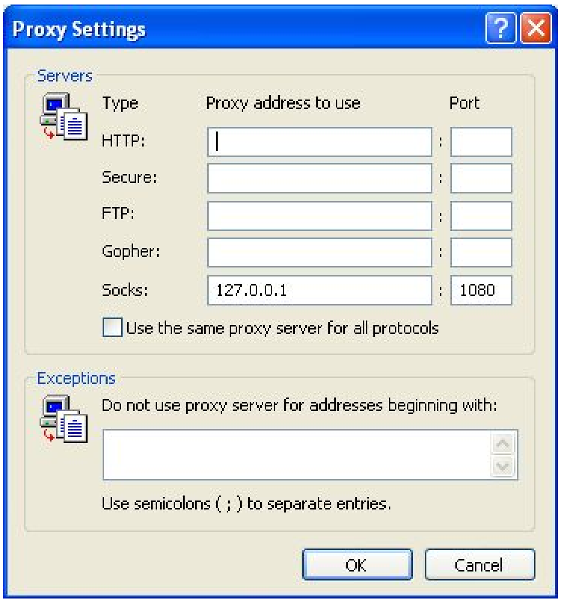
☑ Use the same proxy server for all protocols

Exceptions

Do not use proxy server for addresses beginning with:

Use semicolons (;) to separate entries.

7. Enter the "Proxy address to use" and "Port" number in the "Socks" row and click "OK":



Proxy Settings

Servers

Type	Proxy address to use	Port
HTTP:		
Secure:		
FTP:		
Gopher:		
Socks:	127.0.0.1	1080

☐ Use the same proxy server for all protocols

Exceptions

Do not use proxy server for addresses beginning with:

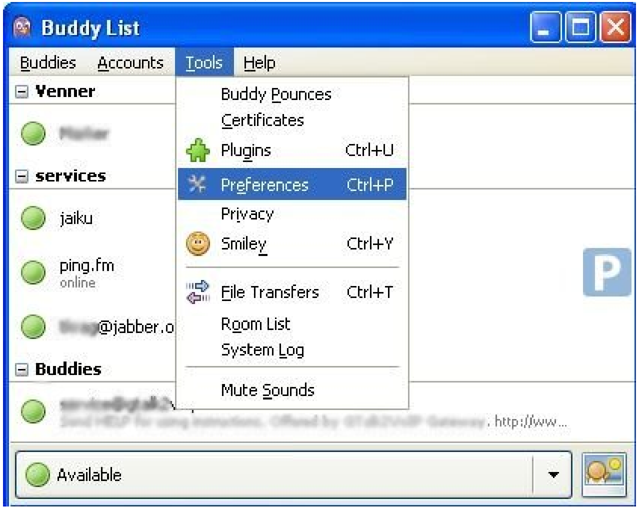
Use semicolons (;) to separate entries.

Now Internet Explorer is configured to use a SOCKS proxy.

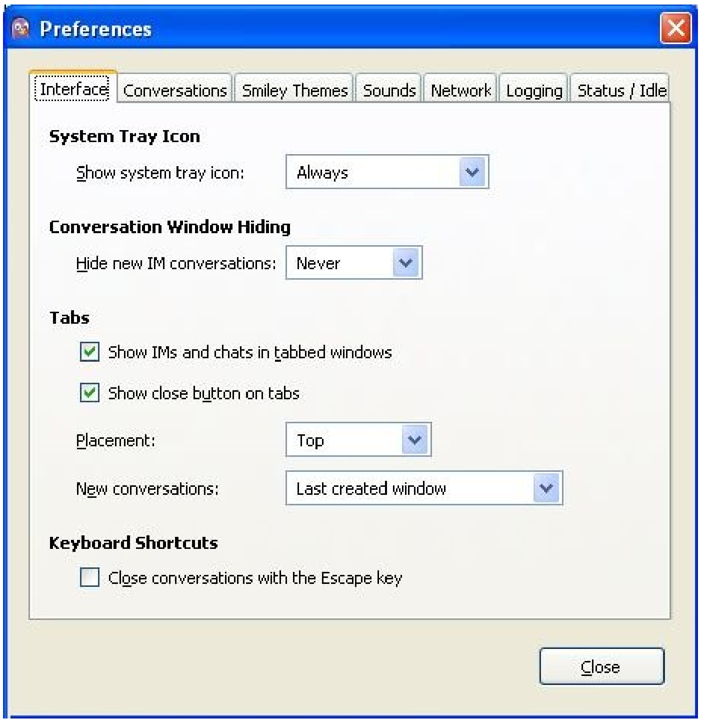
Configuring a SOCKS proxy for other applications

Many Internet applications other than Web browsers can use a SOCKS proxy to connect to the Internet, potentially bypassing blocking. Here is an example with the instant messaging software Pidgin. This is a typical example, but the exact sequence of steps to configure some other application to use a SOCKS proxy would be slightly different.

1. On the "Tools" menu, click "Preferences".



2. Pidgin displays the Preferences window.



Preferences

Interface | Conversations | Smiley Themes | Sounds | Network | Logging | Status / Idle

System Tray Icon

Show system tray icon: Always

Conversation Window Hiding

Hide new IM conversations: Never

Tabs

☑ Show IMs and chats in tabbed windows

☑ Show close button on tabs

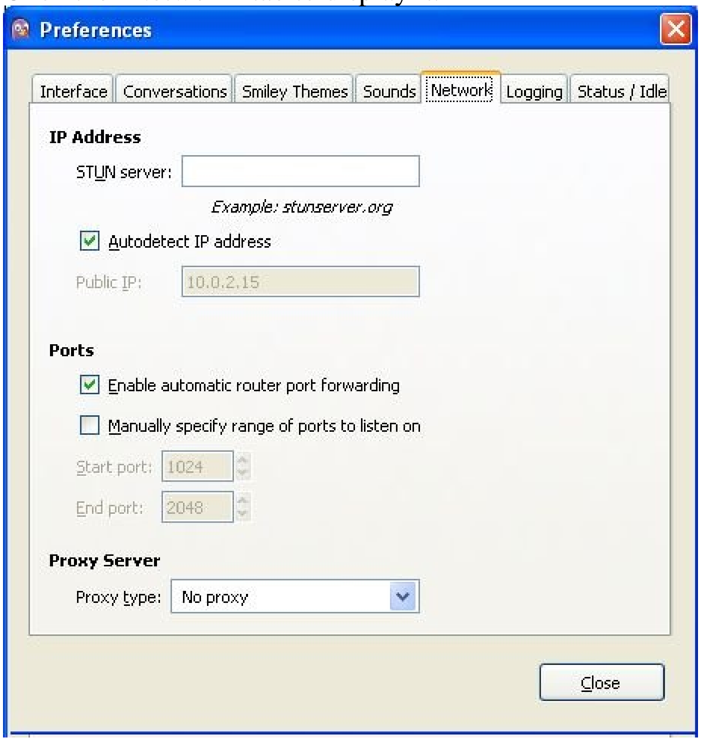
Placement: Top

New conversations: Last created window

Keyboard Shortcuts

□ Close conversations with the Escape key

3. Click the "Network" tab to display it.



Preferences

Interface | Conversations | Smiley Themes | Sounds | Network | Logging | Status / Idle

IP Address

STUN server:

Example: stunserver.org

☑ Autodetect IP address

Public IP: 10.0.2.15

Ports

☑ Enable automatic router port forwarding

□ Manually specify range of ports to listen on

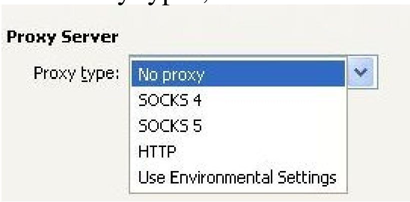
Start port: 1024

End port: 2048

Proxy Server

Proxy type: No proxy

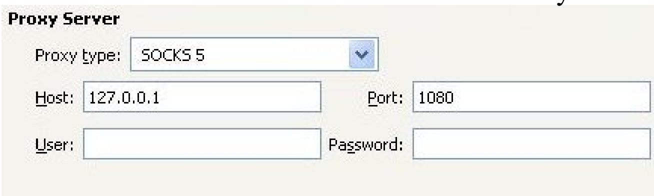
4. For "Proxy type", select "SOCKS 5". Additional fields appear under that option.



Proxy Server

Proxy type: No proxy

5. Enter the "Host" address and "Port" number of your SOCKS proxy.



Proxy Server

Proxy type: SOCKS 5

Host: 127.0.0.1 Port: 1080

User: Password:

6. Click "Close".

Pidgin is now configured to use a SOCKS proxy.

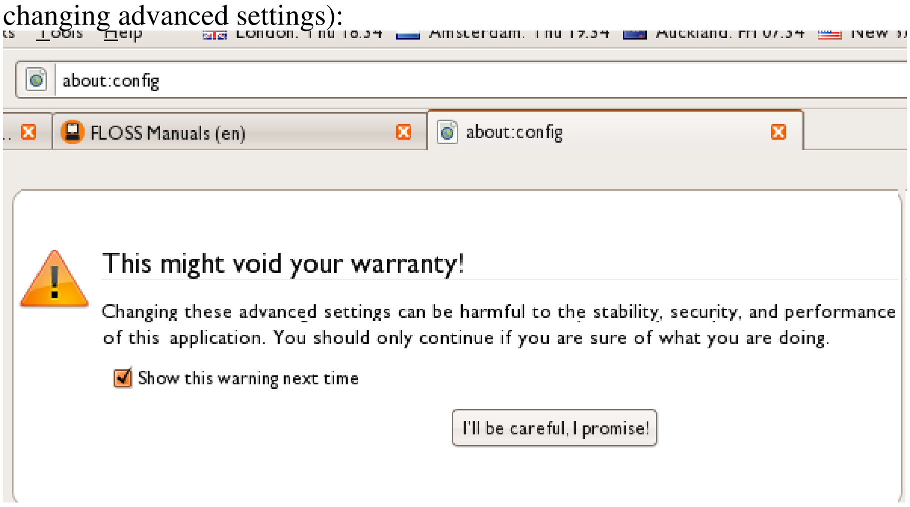
When you're done with the proxy

When you are done using a proxy, particularly on a shared computer, return the settings you've changed to their previous values. Otherwise, those applications will continue to try to use the proxy. This could be a problem if you don't want people to know that you were using the proxy or if you were using a local proxy provided by a particular circumvention application that isn't running all the time.

DNS leaks

One important problem with SOCKS proxies is that some applications that support the use of SOCKS proxies may not use the proxy for all their network communications. The most common problem is that Domain Name System (DNS) requests may be made without going through the proxy. This **DNS leak** can be a privacy problem and can also leave you vulnerable to DNS blocking, which a proxy could otherwise have circumvented. Whether an application is vulnerable to DNS leaks may vary from version to version. Mozilla Firefox is currently vulnerable to DNS leaks in its default configuration, but you can avoid these by making a permanent configuration change to prevent DNS leaks:

1. In the Firefox address bar, enter **`about:config`** as if it were a URL (you may see a warning about changing advanced settings):


Tools Help
London: Thu 16:34 Amsterdam: Thu 17:34 Auckland: Fri 07:34 New Y
about:config
FLOSS Manuals (en)
about:config

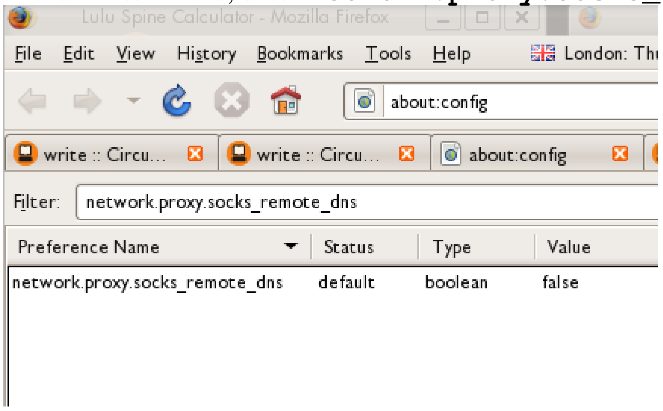
This might void your warranty!

Changing these advanced settings can be harmful to the stability, security, and performance of this application. You should only continue if you are sure of what you are doing.

☑ Show this warning next time

I'll be careful, I promise!

2. If necessary, click "I'll be careful, I promise!" to confirm that you want to modify your browser settings. The browser displays a list of configuration settings information.
3. In the "Filter" field, enter **`network.proxy.socks_remote_dns`**. Only that setting is displayed.


Lulu Spine Calculator - Mozilla Firefox
File Edit View History Bookmarks Tools Help
London: Thu
about:config
write :: Circu...
write :: Circu...
about:config

Filter: network.proxy.socks_remote_dns

Preference Name	Status	Type	Value
network.proxy.socks_remote_dns	default	boolean	false

4. If this setting has the value **false**, double-click it to change its value to **true**.

Firefox is now configured to avoid DNS leaks. Once the value is displayed as **true**, this setting is automatically saved permanently.

There is no documented way to prevent DNS leaks within Microsoft Internet Explorer, without using an external program.

At the time of this writing there are no known DNS leaks in Pidgin when configured to use a SOCKS 5 proxy.

Installing a Web Proxy

Installation of Web-based circumvention software can require some technical expertise and resources (a compatible Web server and sufficient bandwidth).

There are two categories of Web proxies: private and public. With a private Web proxy, the location is only made known to the intended users; public Web proxies are available to anyone interested or to anyone able to locate them. Public Web proxies and anonymity services may be known to both users *and* those implementing filtering, so they are more vulnerable to blacklisting. The chances of private Web proxies being detected and blocked are lower than those of public circumvention services.

Private Web proxies can be set up with some level of customization tailored to the specific needs of the end user. Common customizations would include changing the port number that the Web server runs on and implementing encryption like SSL. Since some blacklists may block keywords associated with popular proxy software, changing items like the default URL, the name of the script, or elements of the user interface can also reduce the risk of automated detection and blocking of the proxy.

When using SSL, it's also useful to create an innocuous Web page at the root of the Web server and conceal the Web proxy with a random path and file name. Although intermediaries may be able to determine the server you are connecting to, they will not be able to determine the requested path because that part of the request is encrypted. For example, if a user connects to https://example.com/secretproxy/, an intermediary will be able to determine that the user connected to example.com but they will not know that the user requested the Web proxy. (If the Web proxy operator places an innocuous page at example.com, then the Web proxy is less likely to be discovered by monitoring network transmissions.)

Here are some popular Web proxy programs:

â ¢ **CGIProxy**: A CGI script that acts as both an HTTP and an FTP proxy.
http://www.jmarshall.com/tools/cgiproxy

â ¢ **Peacefire's Circumventor**: An automated installer program that makes it much easier
for non-technical users to install and configure CGIProxy on a Windows machine.
http://www.peacefire.org/circumventor/simple-circumventor-instructions.html

â ¢ **PHProxy**: A PHP script that acts as both an HTTP and an FTP proxy.
http://sourceforge.net/projects/poxy/

â ¢ **Psiphon**: An automated installer program that makes it much easier
for non-technical users to install and configure PHProxy on a Windows machine.
http://psiphon.civisec.org/

Private Web proxies are best suited for users who require stable circumvention services for Web traffic and have trusted contacts in non-filtered locations with sufficient technical skills and available bandwidth to set up and maintain the Web proxy. This is also the most flexible circumvention option available for simple Web traffic and is less likely to be discovered and blocked than a public Web proxy, particularly if it is used with SSL encryption.

Installing PHProxy

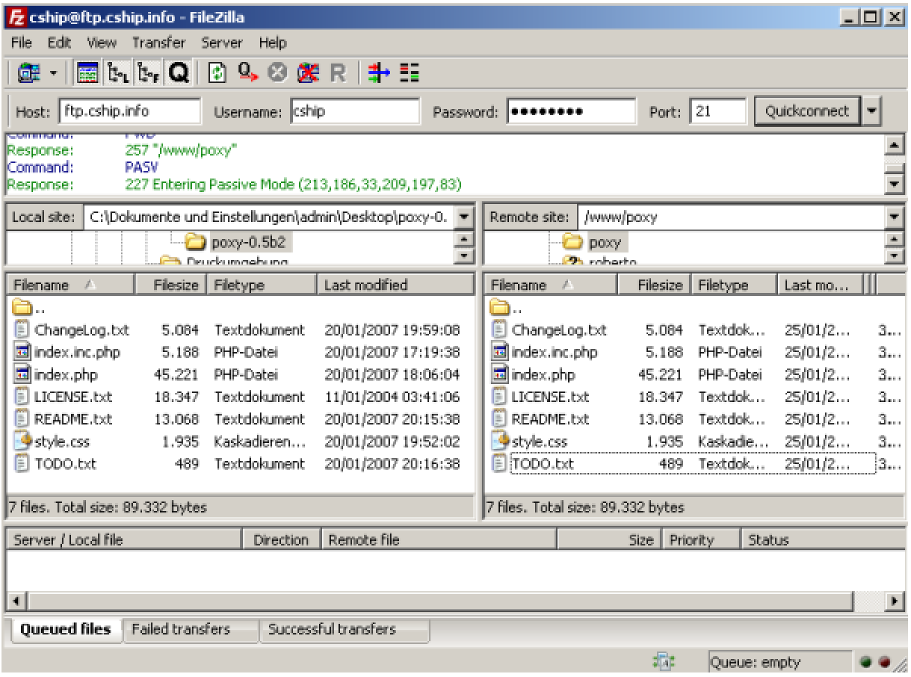
Installing PHProxy requires space on a Web server on an uncensored Internet connection which has PHP support. This can be either:

- Rented Web space (which can be purchased for a few US dollars a year from hosting companies such as http://www.dreamhost.com/)
- A virtual/dedicated server (which are more expensive and more complicated to use)
- A PC connected to a DSL/cable connection (with a publicly routable IP address)
- A PC on a university broadband connection, or an account on a university server (if the university doesn't prohibit this use)

These instructions describe the most common case: using FTP to transfer PHProxy into a Web space account that already supports PHP. For this technique, you will also need an FTP client program such as FileZilla (http://filezilla-project.org/).

Although this method is the most common, it isn't applicable to every situation. For instance, if you're setting up your own server, if your server doesn't support FTP, or if you're familiar with the command-line interface to the server, you might use a different method.

- First, download the PHProxy script from http://sourceforge.net/projects/poxy/. The script is only 25 kilobytes, so it is considerably smaller than most Web sites.
- Next, extract the contents of the .ZIP file by clicking with the right mouse button on the file and choosing "Extract here".
- Start your FTP client, enter the server (host), username and password you got from your Web space provider and click on "Quickconnect".
- The left part of the FTP client window represents your local PC, so locate the PHProxy files you just extracted in here.
- You can then drag-and-drop the files from the left part of the FTP client window to the right part, which represents the remote FTP server (your Web space).



Host: ftp.cship.info   Username: cship   Password: ●●●●●●●●●   Port: 21

```
Response:       257 "/www/poxy"
Command:        PASV
Response:       227 Entering Passive Mode (213,186,33,209,197,83)
```

Local site: C:\Dokumente und Einstellungen\admin\Desktop\poxy-0.

poxy-0.5b2

Filename	Filesize	Filetype	Last modified
..			
ChangeLog.txt	5.084	Textdokument	20/01/2007 19:59:08
index.inc.php	5.188	PHP-Datei	20/01/2007 17:19:38
index.php	45.221	PHP-Datei	20/01/2007 18:06:04
LICENSE.txt	18.347	Textdokument	11/01/2004 03:41:06
README.txt	13.068	Textdokument	20/01/2007 20:15:38
style.css	1.935	Kaskadieren...	20/01/2007 19:52:02
TODO.txt	489	Textdokument	20/01/2007 20:16:38

7 files. Total size: 89.332 bytes

Remote site: /www/poxy

poxy

Filename	Filesize	Filetype	Last mo...	
..				
ChangeLog.txt	5.084	Textdok...	25/01/2...	3...
index.inc.php	5.188	PHP-Datei	25/01/2...	3...
index.php	45.221	PHP-Datei	25/01/2...	3...
LICENSE.txt	18.347	Textdok...	25/01/2...	3...
README.txt	13.068	Textdok...	25/01/2...	3...
style.css	1.935	Kaskade...	25/01/2...	3...
TODO.txt	489	Textdok...	25/01/2...	3...

7 files. Total size: 89.332 bytes

Server / Local file	Direction	Remote file	Size	Priority	Status

- You can now access PHProxy by going to the Domain of your Web space and the directory to which you uploaded PHProxy. (In this example http://www.cship.info/poxy/.)

If this doesn't work, your server account may not support PHP, or support for PHP may be disabled or may require additional steps. Consult the documentation for your account or the Web server software in use. You can also look for an appropriate support forum or ask your web server operator for additional help.

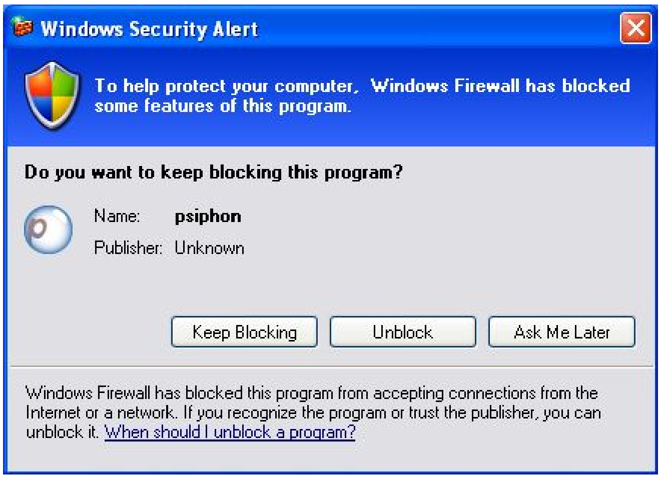
Installing psiphon

In order to create an installation of psiphon you will need a computer with an uncensored Internet connection running Windows. You may also need to set up a **port forwarding** rule in your router to forward port 443 to your Windows computer. How to do this is explained in your router manual or on http://portforward.com/english/applications/port_forwarding/HTTPS/HTTPSindex.htm.

To get started, download the script from http://www.psiphon.ca/download.php (about 2MB).

Double-click the Installer file (ending in ".msi"), click "Next" and choose a directory where psiphon should be installed. If you are not sure, just leave the default folder as is and click "Next".

To start the program, double-click the "psiphon" icon on your desktop. When you do this the first time, you may see a Windows firewall warning. If so, choose "Unblock".



Windows Security Alert

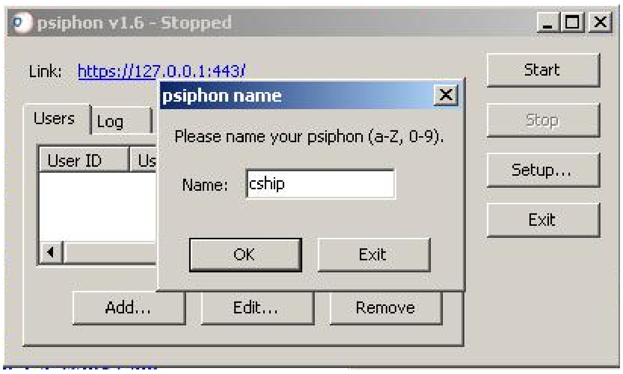
To help protect your computer, Windows Firewall has blocked some features of this program.

Do you want to keep blocking this program?

Name: psiphon
Publisher: Unknown

Windows Firewall has blocked this program from accepting connections from the Internet or a network. If you recognize the program or trust the publisher, you can unblock it. When should I unblock a program?

Then you have to configure your psiphon node. First choose a name for your psiphon node, for example "cship". This name will be part of the URL which you or your buddy will use to access the node.



psiphon v1.6 - Stopped

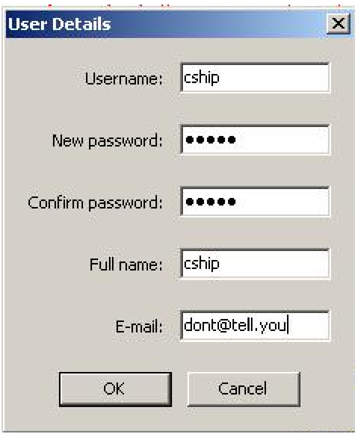
Link: https://127.0.0.1:443/

psiphon name

Please name your psiphon (a-Z, 0-9).

Name: cship

To allow new users to use your psiphon node, you have to create an account for them. To do so, click "Add" and enter the required details.



User Details

Username: cship

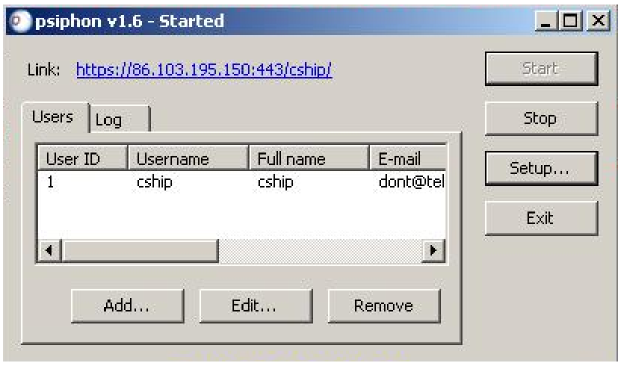
New password: •••••

Confirm password: •••••

Full name: cship

E-mail: dont@tell.you

You can then start your psiphon node by clicking "Start".



psiphon v1.6 - Started

Link: https://86.103.195.150:443/cship/

User ID	Username	Full name	E-mail
1	cship	cship	dont@tel

The program will automatically detect your external IP address and tell you the Link at which other users can access your node. To share the node, provide the link, user name, and password information to your new user.

Setting up a Tor Bridge

If you live in an area with little or no Internet censorship, you may want to run a simple Tor **relay** or a Tor **bridge relay** to help other Tor users access an uncensored Internet.

The Tor network relies on volunteers to donate bandwidth. The more people who run relays, the faster and more secure the Tor network will be. To help people using Tor bypass Internet censorship, set up a bridge relay rather than an ordinary relay.

Bridge relays (or "bridges" for short) are Tor relays that are not listed in the main (and public) Tor directory. Even if an ISP is filtering connections to all the known Tor relays, it probably will not be able to block all the bridges.

What do I need to run a relay or a bridge relay?

There are only a few prerequisites for running a Tor relay:

- Your Internet connection needs to have a bandwidth of at least 20 kilobytes/second in both directions (and it needs to be OK for your connection to be constantly in use when your computer is on).
- You need an Internet connection with an IP address that is publicly routable.
- If your computer is behind a **network address translation (NAT)** firewall and doesn't have access to its public (or external) IP address, you'll need to set up a **port forwarding** rule on your router. You can do this via the Tor Universal Plug and Play facility, or manually, by following the instructions in your router manual or at portforward.com (http://portforward.com/english/applications/port_forwarding/HTTPS/HTTPSindex.htm).

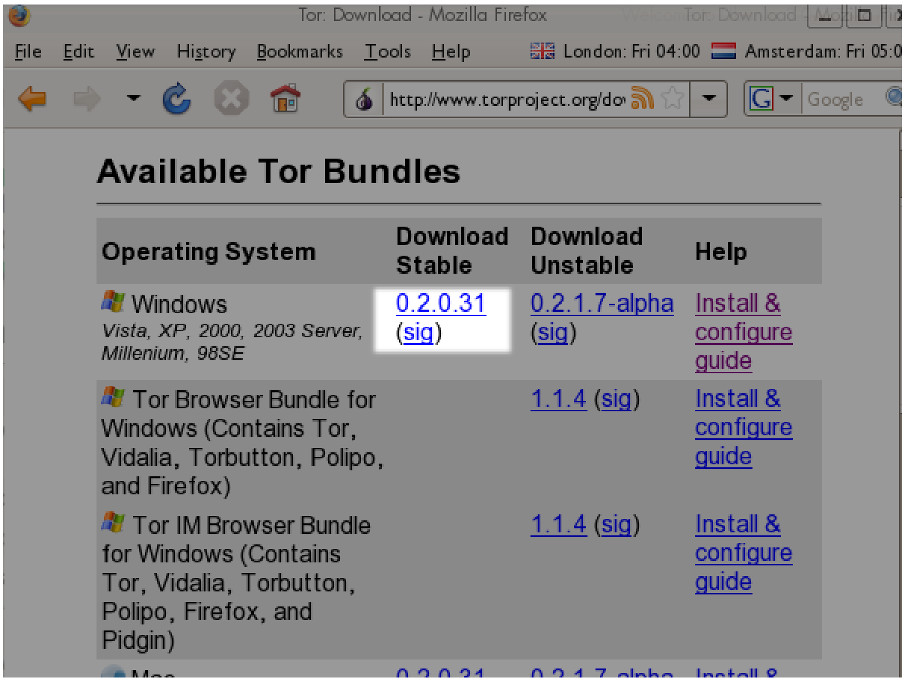
What is *not* required:

- Your computer does not have to be always on and online (the Tor directory will figure out when it is).
- You do not need to have a static IP address.

Downloading Tor

To download Tor, go to the http://www.torproject.org/ Web site and click "Download" in the navigation menu.

On the "Available Tor Bundles" page, select the stable version that fits your operating system.


Tor: Download - Mozilla Firefox
File Edit View History Bookmarks Tools Help
London: Fri 04:00
Amsterdam: Fri 05:0
http://www.torproject.org/do
Google

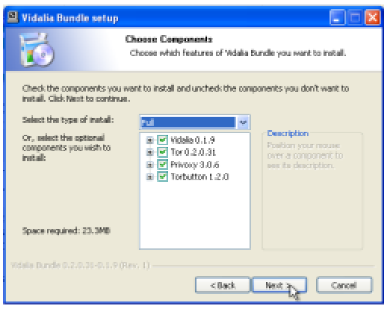
Available Tor Bundles

Operating System	Download Stable	Download Unstable	Help
Windows *Vista, XP, 2000, 2003 Server, Millenium, 98SE*	0.2.0.31 (sig)	0.2.1.7-alpha (sig)	Install & configure guide
Tor Browser Bundle for Windows (Contains Tor, Vidalia, Torbutton, Polipo, and Firefox)		1.1.4 (sig)	Install & configure guide
Tor IM Browser Bundle for Windows (Contains Tor, Vidalia, Torbutton, Polipo, Firefox, and Pidgin)		1.1.4 (sig)	Install & configure guide
Mac	0.2.0.31	0.2.1.7-alpha	Install &

Installing Tor

Launch the installer and click "Next" when asked.

If you are using Firefox, install all the components proposed in the dialog shown below:



Choose Components

Choose which features of Vidalia Bundle you want to install.

Check the components you want to install and uncheck the components you don't want to install. Click Next to continue.

Select the type of install: Full

Or, select the optional components you wish to install:

- ☑ Vidalia 0.1.9
- ☑ Tor 0.2.0.31
- ☑ Privoxy 3.0.6
- ☑ Torbutton 1.2.0

Description

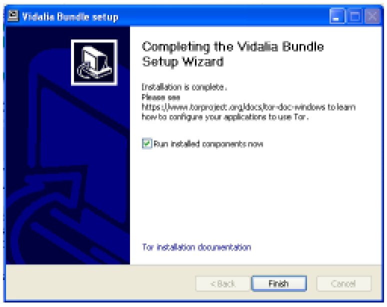
Position your mouse over a component to see its description.

Space required: 23.3MB

Vidalia Bundle 0.2.0.31-0.1.9 (Rev. 1)

If you do not have Firefox installed, deselect "Torbutton" (you will have the option to install Firefox and Torbutton afterwards).

When the installation is completed, launch Tor by clicking "Finish" with the "Run installed components now" box selected, as in the dialog shown below:



Completing the Vidalia Bundle Setup Wizard

Installation is complete.
Please see
https://www.torproject.org/docs/tor-doc-windows to learn how to configure your applications to use Tor.

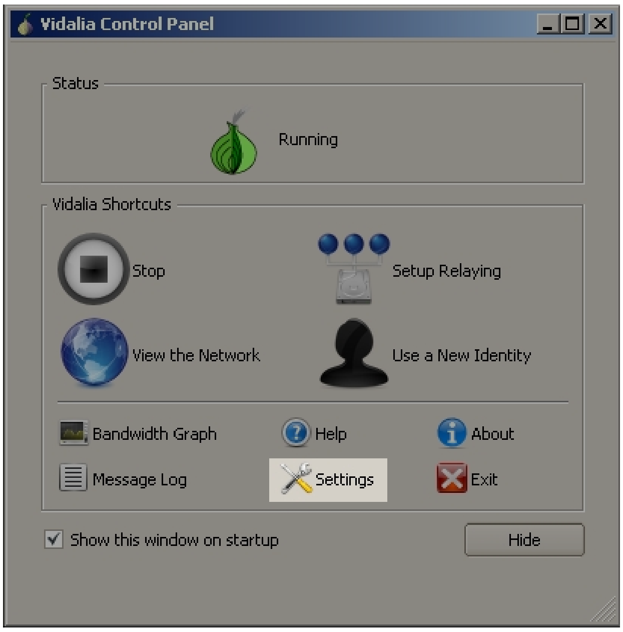
☑ Run installed components now

Tor installation documentation

Configuring Tor to be a bridge

To activate your bridge:

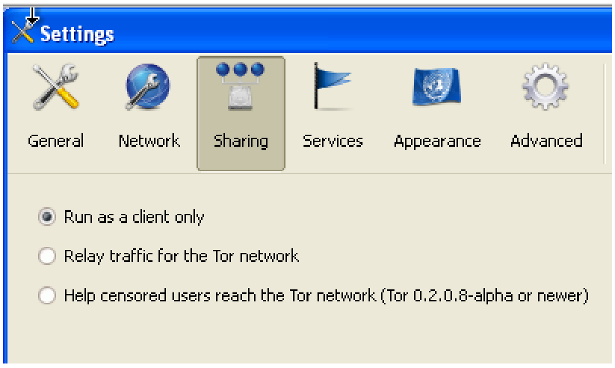
- Open the Vidalia control panel.
- In the Vidalia control panel, click "Settings".



Status: Running

☑ Show this window on startup

- In the "Settings" window, click "Sharing":

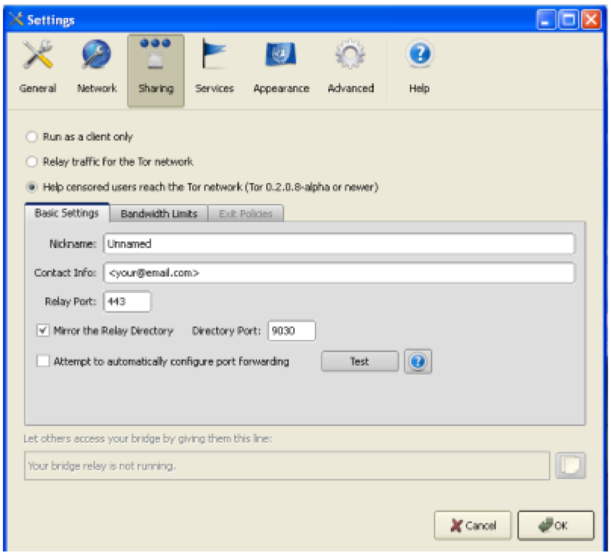


● Run as a client only

○ Relay traffic for the Tor network

○ Help censored users reach the Tor network (Tor 0.2.0.8-alpha or newer)

- To create the bridge, click "Help censored users reach the Tor network".

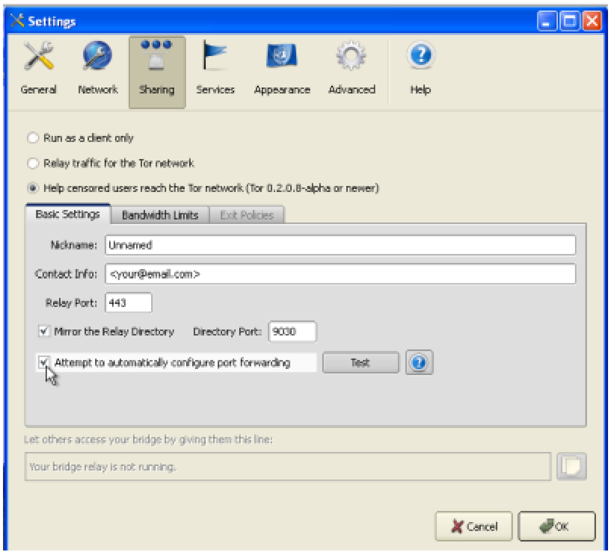


○ Run as a client only
○ Relay traffic for the Tor network
● Help censored users reach the Tor network (Tor 0.2.0.8-alpha or newer)

Nickname: Unnamed
Contact Info: <your@email.com>
Relay Port: 443
☑ Mirror the Relay Directory Directory Port: 9030
□ Attempt to automatically configure port forwarding

Let others access your bridge by giving them this line:
Your bridge relay is not running.

- If you are using a NAT IP address on a local network, you will need to create a **port forwarding** rule in your router. You can ask Tor to try to configure port forwarding for you. To do so, click "Attempt to automatically configure port forwarding".

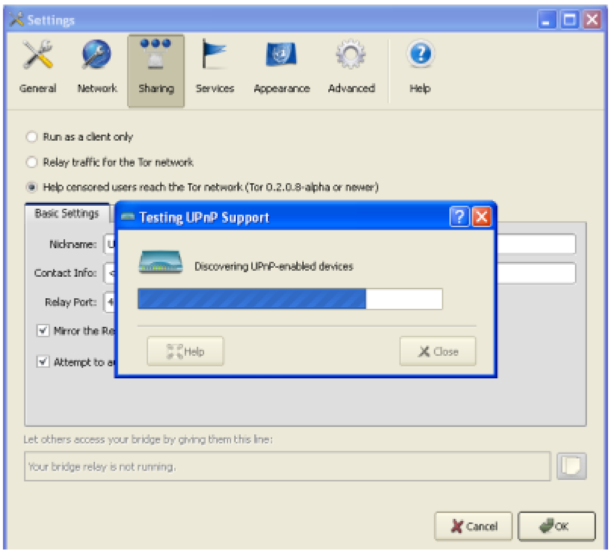


○ Run as a client only
○ Relay traffic for the Tor network
● Help censored users reach the Tor network (Tor 0.2.0.8-alpha or newer)

Nickname: Unnamed
Contact Info: <your@email.com>
Relay Port: 443
☑ Mirror the Relay Directory Directory Port: 9030
☑ Attempt to automatically configure port forwarding

Let others access your bridge by giving them this line:
Your bridge relay is not running.

- Click "Test" to see if Tor correctly created a setting for port forwarding in the router.



○ Run as a client only
○ Relay traffic for the Tor network
● Help censored users reach the Tor network (Tor 0.2.0.8-alpha or newer)

Nickname: U
Contact Info: <
Relay Port: 4
☑ Mirror the Re
☑ Attempt to a

Discovering UPnP-enabled devices

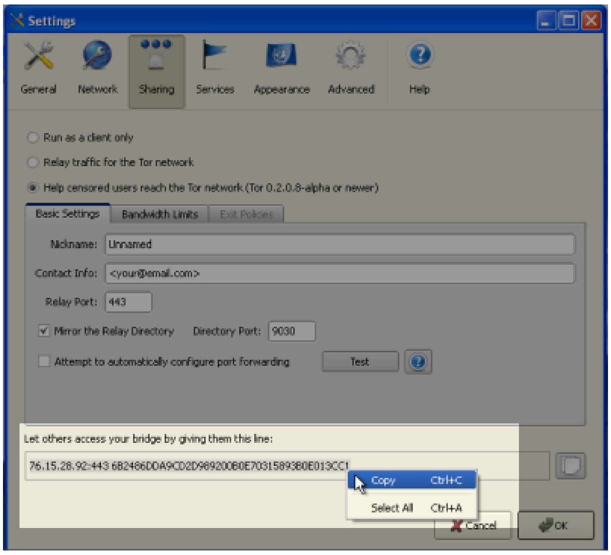
Let others access your bridge by giving them this line:
Your bridge relay is not running.

- If Tor could not configure port forwarding, please read the Tor FAQ entry on this topic: https://wiki.torproject.org/noreply/TheOnionRouter/TorFAQ#ServerForFirewalledClients

Congratulations. If all has gone well, your bridge is up and running. Your bridge information will be added to the hidden bridge directory and made available to users who request it.

Sharing your bridge with friends

If you specifically established your bridge to help a friend access the Tor network, you can copy the information at the bottom of the Settings window and send it to him/her.



○ Run as a client only

○ Relay traffic for the Tor network

● Help censored users reach the Tor network (Tor 0.2.0.8-alpha or newer)

Nickname: Unnamed

Contact Info: <your@email.com>

Relay Port: 443

☑ Mirror the Relay Directory Directory Port: 9030

□ Attempt to automatically configure port forwarding

Let others access your bridge by giving them this line:

76.15.28.92:443 6B2486DDA9CD2D989200B0E7031589380E013CC1

Risks of Operating a Proxy

When you run a Web or **application proxy** on your computer, requests and connections forwarded through that proxy will appear to originate from your computer. So if someone uses the proxy to send or receive material that a third party objects to, you could receive complaints that assume that you are responsible and may ask you to stop that activity. In some cases, activities using your proxy could attract legal action or the attention of law enforcement agencies in your own or another country.

In some countries, proxy operators have received legal complaints, and, in some cases, law enforcement agents have seized computers that were functioning as proxies. This could happen for several reasons:

- Someone may wrongly assume that the operator of the proxy computer was personally involved in activity passing through the proxy.
- Someone may assert that the operator of the proxy has a legal duty to stop certain uses.
- Someone may hope to examine the proxy to find evidence (e.g. logfiles) of who was responsible for some activity.

If you think this could be a risk for your proxy in your area, it may be safer to operate the proxy on a dedicated computer in a data center.

National laws may vary in the way and extent they protect proxy operators from liability. For details about your situation, you should consult a lawyer or qualified legal expert in your jurisdiction.

Internet service providers may also complain about your operation of a proxy, especially if they receive complaints about abuse of the proxy. Some **ISP**s may assert that running a **public proxy** violates their terms of service, or that they simply do not wish to permit users to run public proxies. These ISPs may disconnect you or threaten to disconnect you in the future.

Risks of operating a non-public proxy

These risks still exist if you operate a proxy for your own benefit or for the use of a small number of individuals, but operating a non-public proxy is much less risky than operating a public proxy.

If the user of your non-public proxy is detected and monitored, whoever is doing the monitoring may realize or speculate that there is a connection between you and the user and that you are trying to help that person circumvent filtering.

Although your own ISP is much more likely to object to your running a public proxy than a private proxy, some ISPs may have such comprehensive anti-proxy policies that they object even to the operation of a private proxy on their networks.

Risks of operating a Tor node (Tor relay)

A **Tor node** is a kind of public proxy, so running one can have the risks described above. However, a Tor node is typically set up in one of two ways: as an **exit node** or as a **middleman node** (sometimes called a **non-exit node**). A middleman node forwards encrypted traffic only to other Tor nodes, and does not allow anonymous users to communicate directly with sites outside of the Tor network. Running either kind of node is helpful to the Tor network as a whole. Running an exit node is particularly helpful because exit nodes are comparatively scarce. Running a middleman node is comparatively less risky because the middleman node is unlikely to draw the kinds of complaints that a public proxy might, since the IP address of a middleman node will never appear on log files.

Another Tor node configuration, called a **bridge**, is available specifically to help other users circumvent Internet censorship. Since a bridge is not an exit node, you are unlikely to receive complaints about the use of a bridge node by others.

Even though it is unlikely to draw specific complaints, operating a middleman or bridge node may cause your Internet service provider to object for more general reasons. For example, the ISP may disapprove of the Tor network or may forbid subscribers from operating any sort of public service.

Data retention laws might regulate proxy operation

In some countries, **data retention laws** or similar laws meant to restrict anonymity might be interpreted to regulate the operation of proxy services. For more information about data retention, see http://en.wikipedia.org/wiki/Telecommunications_data_retention.

Resources

Bypassing Internet Censorship is a big topic, with dozens of tools and services available. There are also lots of things to consider if you want your **circumvention** activities to be harder to detect or to **block** in the future, if you want to achieve anonymity in your Internet use, or if you want to help other people circumvent censorship. Here are some recommended resources for further study about related matters. (Some of these resources may be unavailable or blocked in some places.)

Manuals and guides

Circumventing Internet censorship

- Everyone's Guide to By-Passing Internet Censorship for Citizens Worldwide, Citizen Lab, http://www.civisec.org/guides/everyones-guides
- Reporters Without Borders, *Handbook for Bloggers and Cyber-Dissidents,* available at http://www.rsf.org/article.php3?id_article=26187
- The Internet Censorship Wiki: http://en.cship.org/wiki/

Computer security advice for activists

- NGO-in-a-Box, a collection of free portable applications: http://security.ngoinabox.org/
- Digital Security and Privacy for Human Rights Defenders: http://www.frontlinedefenders.org/manual/en/esecman/

Studies on Internet Censorship

- Ronald Deibert, John Palfrey, Rafal Rohozinski, Jonathan Zittrain*, Access Denied: The Practice and Policy of Global Internet Filtering* (Cambridge, MA: MIT Press, 2008), ISBN 0-262-54196-3, available at http://www.opennet.net/accessdenied/
- More resources on Internet Censorship: http://bailiwick.lib.uiowa.edu/journalism/mediaLaw/cyber_censors.html

Organizations that work on documenting, fighting or circumventing Internet restrictions

- Amnesty International campaign to combat Internet repression (http://irrepressible.info)
- Citizen Lab (http://www.citizenlab.org/) and Civisec Project (http://www.civisec.org/)
- Committee to Protect Bloggers (http://www.committeetoprotectbloggers.org/)
- Berkman Center for Internet and Society (http://cyber.law.harvard.edu/)
- Electronic Frontier Foundation (http://www.eff.org/)
- FrontLine (http://www.frontlinedefenders.org/)
- Global Internet Freedom Consortium (http://www.internetfreedom.org/)
- The Herdict (http://www.herdict.org/NetworkHealthAbout.jsp?_sourcePage=%2FPCHealthDownload.jsp)
- OpenNet Initiative (http://opennet.net/)
- Peacefire (http://www.peacefire.org/)
- Reporters Sans FrontiÃ¨res/Reporters Without Borders (http://www.rsf.org/)
- Sesawe (https://sesawe.net)
- Tactical Tech Collective (http://www.tacticaltech.org/)

Open Web proxies and application proxies

- Proxy.org, a list of thousands of open Web Proxies: http://www.proxy.org/
- Subscribe to http://www.peacefire.org/circumventor/, a mailinglist which sends out new web proxies weekly
- Application proxies:
    - http://www.dmoz.org/Computers/Internet/Proxying_and_Filtering/Hosted_Proxy_Services/Free/Proxy
    - http://www.publicproxyservers.com/

Circumvention solutions and service operators

- Access Flickr!: https://addons.mozilla.org/en-US/firefox/addon/4286
- Anonymizer Anonymous Surfing: http://www.anonymizer.com/
- CECID: http://cecid.labyrinthdata.net.au/
- Circumventor CGIProxy: http://peacefire.org/circumventor/
- Codeen: http://codeen.cs.princeton.edu/
- Coral: http://www.coralcdn.org/
- CProxy: http://www.cproxy.com/
- Dijjer: http://dijjer.org/
- Dynaweb FreeGate: http://www.dit-inc.us/freegate
- FirePhoenix: http://firephoenix.edoors.com/
- FreeAccess Plus!: https://addons.mozilla.org/en-US/firefox/addon/6139
- FoxyProxy: http://foxyproxy.mozdev.org/
- Glype: http://www.glype.com/
- GPass: http://gpass1.com/gpass/
- GProxy: http://gpass1.com/gproxy.php
- Gtunnel: http://gardennetworks.org/products
- Guardster: http://www.guardster.com/
- Hamachi LogMeIn: https://secure.logmein.com/products/hamachi/vpn.asp
- hopster: http://www.hopster.com/
- HotSpotVPN: http://hotspotvpn.com/
- httpTunnel: http://www.http-tunnel.com/
- JAP / JonDo: http://www.jondos.de/en
- Megaproxy: http://www.megaproxy.com/
- OpenVPN: http://www.openvpn.net/
- PHProxy: http://sourceforge.net/projects/poxy/
- Picidae: http://www.picidae.net/
- Proxify: http://proxify.com/
- psiphon: http://www.psiphon.ca/
- PublicVPN: http://www.publicvpn.com/
- SmartHide: http://www.smarthide.com/
- SwitchProxy Tool: https://addons.mozilla.org/en-US/firefox/addon/125
- Tor: http://torproject.org
- TrafficCompressor: http://www.tcompressor.ru/
- UltraReach UltraSurf: http://www.ultrareach.com/
- VPNBegir: http://www.vpnbegir.com/
- Your-Freedom: http://www.your-freedom.net/
- Zelune: http://www.zelune.net/

A list of commercial VPN providers

- http://en.cship.org/wiki/VPN

Socksification softwares

- tsocks: http://tsocks.sourceforge.net/
- WideCap: http://www.widecap.com/
- ProxyCap: http://www.proxycap.com/
- FreeCap: http://www.freecap.ru/eng/
- Proxifier: http://www.proxifier.com/
- SocksCap: http://soft.softoogle.com/ap/sockscap-download-5157.shtml

Glossary

Much of this content is based on http://en.cship.org/wiki/Special:Allpages

aggregator

An aggregator is a service that gathers syndicated information from one or many sites and makes it available at a different address. Sometimes called an RSS aggregator, a feed aggregator, a feed reader, or a news reader. (Not to be confused with a Usenet News reader.)

anonymity

Anonymity on the Internet is the ability to use services without leaving clues to one's identity. The level of protection depends on the anonymity techniques used and the extent of monitoring. The strongest techniques in use to protect anonymity involve creating a chain of communication using a random process to select some of the links, in which each link has access to only partial information about the process. The first knows the user's IP address but not the content, destination, or purpose of the communication, because the message contents and destination information are encrypted. The last knows the identity of the site being contacted, but not the source of the session. One or more steps in between prevents the first and last links from sharing their partial knowledge in order to connect the user and the target site.

anonymous remailer

An anonymous remailer is a service that accepts e-mail messages containing instructions for delivery, and sends them out without revealing their sources. Since the remailer has access to the user's address, the content of the message, and the destination of the message, remailers should be used as part of a chain of *multiple* remailers so that no one remailer knows all this information.

ASP (application service provider)

An ASP is an organization that offers software services over the Internet, allowing the software to be upgraded and maintained centrally.

backbone

A backbone is one of the high-bandwidth communications links that tie together networks in different countries and organizations around the world to form the Internet.

badware

See malware.

bandwidth

The bandwidth of a connection is the maximum rate of data transfer on that connection, limited by its capacity and the capabilities of the computers at both ends of the connection.

bash (Bourne-again shell)

The bash shell is a command-line interface for Linux/Unix operating system, based on the Bourne shell.

BitTorrent

BitTorrent is a peer-to-peer file-sharing protocol invented by Bram Cohen in 2001. It allows individuals to cheaply and effectively distribute large files, such as CD images, video, or music files.

blacklist

A blacklist is a list of forbidden persons or things. In Internet censorship, lists of forbidden Web sites may be used as blacklists; censorware may allow access to all sites except for those specifically listed on its blacklist. An alternative to a blacklist is a "whitelist", or a list of permitted things. A whitelist system blocks access to all sites except for those specifically listed on the whitelist. This is a less common approach to Internet censorship. It is possible to combine both approaches, using string matching or other conditional techniques on URLs that do not match either list.

block

To block is to prevent access to an Internet resource, using any number of methods.

bookmark

A bookmark is a placeholder within software that contains a reference to an external resource. In a browser, a bookmark is a reference to a Web page - by choosing the bookmark you can quickly load the Web site without needing to type in the full URL.

bridge

See Tor bridge.

cache

A cache is a part of an information-processing system used to store recently used or frequently used data to speed up repeated access to it. A Web cache holds copies of Web page files.

censor

To censor is to prevent publication or retrieval of information, or take action, legal or otherwise, against publishers and readers.

censorware

Censorware is software used to filter or block access to the Internet. This term is most often used to refer to Internet filtering or blocking software installed on the client machine (the PC which is used to access the Internet). Most such client-side censorware is used for parental control purposes.

Sometimes the term "censorware" is also used to refer to software used for the same purpose installed on a network server or router.

CGI (Common Gateway Interface)

CGI is a common standard used to let programs on a Web server run as Web applications. Many Web-based proxies use CGI and thus are also called "CGI proxies". (One popular CGI proxy application written by James Marshall using the Perl programming language is called CGIProxy.)

chat

Chat, also called Instant Messaging, is a common method of communication among two or more people in which each line typed by a participant in a session is echoed to all of the others. There are numerous chat protocols, including those created by specific companies (AOL, Yahoo!, Microsoft, and others) and publicly defined protocols. Some chat client software use only one of these protocols, while others use a range of popular protocols.

circumvention

Circumvention is publishing or accessing content in spite of attempts at censorship. Also, avoiding surveillance while doing so.

Common Gateway Interface

See CGI.

command-line interface

A method of controlling the execution of software using commands entered on a keyboard, such as a Unix shell or the Windows command line.

cookie

A cookie is a text string sent by a Web server to the user's browser to store on the user's computer, containing information needed to maintain continuity in sessions across multiple Web pages, or across multiple sessions. Some Web sites cannot be used without accepting and storing a cookie. Some people consider this an invasion of privacy or a security risk.

country code top-level domain (ccTLD)

Each country has a two-letter country code, and a TLD based on it, such as .ca for Canada; this domain is called a country code top-level domain. Each such ccTLD has a DNS server that lists all second-level domains within the TLD. The Internet root servers point to all TLDs, and cache frequently-used information on lower-level domains.

DARPA (Defense Advanced Projects Research Agency)

DARPA is the successor to ARPA, which funded the Internet and its predecessor, the ARPAnet.

decryption

Decryption is recovering plain text or other messages from encrypted data with the use of a key.

See also encryption.

domain

A domain can be a Top-Level Domain (TLD) or secondary domain on the Internet.

See also Top-Level Domain, country code Top-Level Domain and secondary domain.

DNS (Domain Name System)

The Domain Name System (DNS) converts domain names, made up of easy-to-remember combinations of letters, to IP addresses, which are hard-to-remember strings of numbers. Every computer on the Internet has an unique address (a little bit like an area code+telephone number).

DNS leak

A DNS leak occurs when a computer configured to use a proxy for its Internet connection nonetheless makes DNS queries without using the proxy, thus exposing the user's attempts to connect with blocked sites. Some Web browsers have configuration options to force the use of the proxy.

DNS server

A DNS server, or name server, is a server that provides the look-up function of the Domain Name System. It does this either by accessing an existing cached record of the IP address of a specific domain, or by sending a request for information to another name server.

DNS tunnel

A DNS tunnel is a way to tunnel almost everything over DNS/Nameservers.

Because you "abuse" the DNS system for an unintended purpose, it only allows a very slow connection of about 3 kb/s which is even less than the speed of an analog modem. That is not enough for YouTube or Filesharing, but should be sufficient for Instant Messengers like ICQ or MSN Messenger and also for plain text e-mail.

On the connection you want to use a DNS tunnel you only need port 53 to be open. So it even works on many commercial WiFi providers without the need to pay.

The main problem is that there are no public modified nameservers that you can use. You have to set up your own. You need a server with a permanent connection to the Internet running Linux. There you can install the free software OzymanDNS and in combination with SSH and a proxy like Squid you can use the tunnel. More Information on this on http://www.dnstunnel.de/

eavesdropping

Eavesdropping is listening to voice traffic or reading or filtering data traffic on a telephone line or digital data connection, usually to detect or prevent illegal or unwanted activities or to control or monitor what people are talking about.

e-mail

E-mail, short for electronic mail, is a method to send and receive messages over the Internet. It is possible to use a Web mail service or to send e-mails with the SMTP protocol and receive them with the POP3 protocol by using an e-mail client like Outlook Express or Thunderbird. It is comparatively rare for a government to block e-mail, but e-mail surveillance is common. If e-mail is not encrypted, it could be read easily by a network operator or government.

encryption

Encryption is any method for recoding and scrambling data or transforming it mathematically to make it unreadable to a third party who doesn't know the secret key to decrypt it. It is possible to encrypt data on your local hard drive using software like TrueCrypt (http://www.truecrypt.org/) or to encrypt Internet traffic with SSL or SSH.

See also decryption.

exit node

An exit node is a Tor node that forwards data outside the Tor network.

See also middleman node.

file sharing

File sharing refers to any computer system where multiple people can use the same information, but often refers to making music, films or other materials available to others free of charge over the Internet.

file spreading engine

A file spreading engine is a Web site a publisher can use to get around censorship. A user only has to upload a file to publish once and the file spreading engine uploads that file to some set of sharehosting services (like Rapidshare or Megaupload).

filter

To filter is to search in various ways for specific data patterns to block or permit communications.

Firefox

Firefox is the most popular free and open source Web browser, developed by the Mozilla Foundation.

forum

On a Web site, a forum is a place for discussion, where users can post messages and comment on previously posted messages. It is distinguished from a mailing list or a Usenet newsgroup by the persistence of the pages containing the message threads. Newsgroup and mailing list archives, in contrast, typically display messages one per page, with navigation pages listing only the headers of the messages in a thread.

frame

A frame is a portion of a Web page with its own separate URL. For example, frames are frequently used to place a static menu next to a scrolling text window.

FTP (File Transfer Protocol)

The FTP protocol is used for file transfers. Many users use it mostly for downloads; it can also be used to upload Web pages and scripts to some Web servers. It normally uses ports 20 and 21, which are sometimes blocked. Some FTP servers listen to an uncommon port, which can evade port-based blocking.

A popular free and open source FTP client for Windows is FileZilla. There are also some Web-based FTP clients that you can use with a normal Web browser like Firefox.

gateway

A gateway is a node connecting two networks on the Internet. An important example is a national gateway that requires all incoming or outgoing traffic to go through it.

honeypot

A honeypot is a site that pretends to offer a service in order to entice potential users to use it, and to capture information about them or their activities.

hop

A hop is a link in a chain of packet transfers from one computer to another, or any computer along the route. The number of hops between computers can give a rough measure of the delay (latency) in communications between them. Each individual hop is also an entity that has the ability to eavesdrop on, block, or tamper with communications.

HTTP (Hypertext Transfer Protocol)

HTTP is the fundamental protocol of the World Wide Web, providing methods for requesting and serving Web pages, querying and generating answers to queries, and accessing a wide range of services.

HTTPS (Secure HTTP)

Secure HTTP is a protocol for secure communication using encrypted HTTP messages. Messages between client and server are encrypted in both directions, using keys generated when the connection is requested and exchanged securely. Source and destination IP addresses are in the headers of every packet, so HTTPS cannot hide the fact of the communication, just the contents of the data transmitted and received.

IANA (Internet Assigned Numbers Authority)

IANA is the organization responsible for technical work in managing the infrastructure of the Internet, including assigning blocks of IP addresses for top-level domains and licensing domain registrars for ccTLDs and for the generic TLDs, running the root name servers of the Internet, and other duties.

ICANN (Internet Corporation for Assigned Names and Numbers)

ICANN is a corporation created by the US Department of Commerce to manage the highest levels of the Internet. Its technical work is performed by IANA.

Instant Messaging (IM)

Instant Messaging is either certain proprietary forms of chat using proprietary protocols, or chat in general. Common Instant Messaging clients include MSN Messenger, ICQ, AIM or Yahoo! Messenger.

intermediary

See man in the middle.

Internet

The Internet is a network of networks interconnected using TCP/IP and other communication protocols.

IP (Internet Protocol) Address

An IP address is a four-byte number (in the current version 4 of the Internet Protocol), identifying a particular computer on the Internet, often represented as four integers in the range 0-255 separated by dots, such as 74.54.30.85.

IRC (Internet relay chat)

IRC is a more than 20-year-old Internet protocol used for real-time text conversations (chat). There exist several IRC networks -- the largest have more than 50 000 users.

ISP (Internet Service Provider)

An ISP (Internet service provider) is a business or organization that provides access to the Internet for its customers.

Javascript

Javascript is a scripting language, commonly used in Web pages to provide interactive functions.

keyword filter

A keyword filter scans all Internet traffic going through a server for forbidden words or terms to block.

log file

A log file is a file that records a sequence of messages from a software process, which can be an application or a component of the operating system. For example, Web servers or proxies may keep log files containing records about which IP addresses used these services when and what pages were accessed.

low-bandwidth filter

A low-bandwidth filter is a Web service that removes extraneous elements such as advertising and images from a Web page and otherwise compresses it, making page download much quicker.

malware

Malware is a general term for malicious software, including viruses, that may be installed or executed without your knowledge. Malware may take control of your computer for purposes such as sending spam. (Malware is also sometimes called badware.)

man in the middle

A man in the middle or man-in-the-middle is a person or computer capturing traffic on a communication channel, especially to selectively change or block content in a way that undermines cryptographic security. Generally the man-in-the-middle attack involves impersonating a Web site, service, or individual in order to record or alter communications. Governments can run man-in-the-middle attacks at country gateways where all traffic entering or leaving the country must pass.

middleman node

A middleman node is a Tor node that is not an exit node. Running a middleman node can be safer than running an exit node because a middleman node will not show up in third parties' log files. (A middleman node is sometimes called a non-exit node.)

monitor

To monitor is to check a data stream continuously for unwanted activity.

network address translation (NAT)

NAT is a router function for hiding an address space by remapping. All traffic going out from the router then uses the router's IP address, and the router knows how to route incoming traffic to the requestor. NAT is frequently implemented by firewalls. Because incoming connections are normally forbidden by NAT, NAT makes it difficult to offer a service to the general public, such as a Web site or public proxy. On a network where NAT is in use, offering such a service requires some kind of firewall configuration or NAT traversal method.

network operator

A network operator is a person or organization who runs or controls a network and thus is in a position to monitor, block, or alter communications passing through that network.

node

A node is an active device on a network. A router is an example of a node. In the psiphon and Tor networks, a server is referred to as a node.

non-exit node

See middleman node.

obfuscation

Obfuscation means obscuring text using easily-understood and easily-reversed transformation techniques that will withstand casual inspection but not cryptanalysis, or making minor changes in text strings to prevent simple matches. Web proxies often use obfuscation to hide certain names and addresses from simple text filters that might be fooled by the obfuscation. As another example, any domain name can optionally contain a final dot, as in "somewhere.com.", but some filters might search only for "somewhere.com" (without the final dot).

packet

A packet is a data structure defined by a communication protocol to contain specific information in specific forms, together with arbitrary data to be communicated from one point to another. Messages are broken into pieces that will fit in a packet for transmission, and reassembled at the other end of the link.

peer-to-peer

A peer-to-peer (or P2P) network is a computer network between equal peers. Unlike client-server networks there is no central server and so the traffic is distributed only among the clients.This technology is mostly applied to **file sharing** programs like **BitTorrent**, eMule and Gnutella. But also the very old **Usenet** technology or the **VoIP** program Skype can be categorized as peer-to-peer systems.

See also file sharing.

PHP

PHP is a scripting language designed to create dynamic Web sites and web applications. It is installed on a Web server. For example, the popular Web proxy "PHProxy" uses this technology.

plain text

Plain text is unformatted text consisting of a sequence of character codes, as in ASCII plain text or Unicode plain text.

plaintext

Plaintext is unencrypted text, or decrypted text.

See also Encryption, SSL, SSH.

privacy

Protection of personal privacy means preventing disclosure of personal information without the permission of the person concerned. In the context of circumvention, it means preventing observers from finding out that a person has sought or received information that has been blocked or is illegal in the country where that person is at the time.

POP3

Post Office Protocol version 3 is used to receive mail from a server, by default on port 110 with an e-mail program like Outlook Express or Thunderbird.

port

A hardware port on a computer is a physical connector for a specific purpose, using a particular hardware protocol. Examples are a VGA display port or a USB connector. Software ports also connect computers and other devices over networks using various protocols, but they exist in software only as numbers. **Ports** are somewhat like numbered doors into different rooms, each for a special service on a server or PC. They are identified by numbers from 0 to 65535.

protocol

A formal definition of a method of communication, and the form of data to be transmitted to accomplish it. Also, the purpose of such a method of communication. For example, Internet Protocol (IP) for transmitting data packets on the Internet, or Hypertext Transfer Protocol for interactions on the World Wide Web.

proxy server

A proxy server is a server, a computer system or an application program which acts as a gateway between a client and a Web server. A client connects to the proxy server to request a Web page from a different server. Then the proxy server accesses the resource by connecting to the specified server, and returns the information to the requesting site. Proxy servers can serve many different purposes, including restricting Web access or helping users route around obstacles.

publicly routable IP address

Publicly routable IP addresses (sometimes called public IP addresses) are those reachable in the normal way on the Internet, through a chain of routers. Some IP addresses are private, such as the 192.168.x.x block, and many are unassigned.

regular expression

A regular expression (also called a regexp or RE) is a text pattern that specifies a set of text strings in a particular regular expression implementation such as the Unix grep utility. A text string "matches" a regular expression if the string conforms to the pattern, as defined by the regular expression syntax. In each RE syntax, some characters have special meanings, to allow one pattern to match multiple other strings. For example, the regular expression `lo+se` matches **`lose,`** **`loose,`** and **`looose.`**

remailer

An anonymous remailer is a service which allows users to send emails anonymously. The remailer receives messages via **e-mail** and forwards them to their intended recipient after removing information that would identify the original sender. Some also provide an anonymous return address that can be used to reply to the original sender without disclosing her identity. Well-known Remailer services include Cypherpunk, Mixmaster and Nym.

router

A router is a computer that determines the route for forwarding packets. It uses address information in the packet header and cached information on the server to match address numbers with hardware connections.

root name server

A root name server or root server is any of thirteen server clusters run by IANA to direct traffic to all of the **TLD**s, as the core of the **DNS** system.

RSS (Real Simple Syndication)

RSS is a method and protocol for allowing Internet users to subscribe to content from a Web page, and receive updates as soon as they are posted.

scheme

On the Web, a scheme is a mapping from a name to a protocol. Thus the HTTP scheme maps URLs that begin with HTTP: to the Hypertext Transfer Protocol. The protocol determines the interpretation of the rest of the URL, so that http://www.example.com/dir/content.html identifies a Web site and a specific file in a specific directory, and mailto:user@somewhere.com is an e-mail address of a specific person or group at a specific domain.

shell

A Unix **shell** is the traditional command line user interface for the Unix/Linux operating systems. The most common shells are sh and **bash**.

SOCKS

A **SOCKS** proxy is a special kind of proxy server. In the ISO/OSI model it operates between the application layer and the transport layer. The standard port for Socks proxies is 1080, but they can also run on different ports. Many programs support a connection through a Socks proxy. If not you can install a Socks client like FreeCap, ProxyCap or SocksCap which can force programs to run through the Socks proxy using dynamic port forwarding. It is also possible to use **SSH** tools such as OpenSSH as a Socks proxy server.

script

A script is a program, usually written in an interpreted, non-compiled language such as Javascript, Java, or a command interpreter language such as bash. Many Web pages include scripts to manage user interaction with a Web page, so that the server does not have to send a new page for each change.

spam

Spam is messages that overwhelm a communications channel used by people, most notably commercial advertising sent to large numbers of individuals or discussion groups. Most such spam advertises products or services that are illegal in one or more ways, almost always including fraud. Content filtering of e-mail to block spam, with the permission of the recipient, is almost universally approved of.

SSH (Secure Shell)

SSH or Secure Shell is a network protocol that allows encrypted communication between computers. It was invented as a successor of the unencrypted Telnet protocol and is also used to access a shell on a remote server.

The standard SSH port is 22. It can be used to bypass Internet censorship with port forwarding or it can be used to tunnel other programs like VNC.

SSL (Secure Sockets Layer)

SSL (or Secure Sockets Layer), is one of several cryptographic standards used to make Internet transactions secure. It is was used as the basis for the creation of the related Transport Layer Security (TLS). You can easily see if you are using SSL/TLS by looking at the URL in your Browser (like Firefox or Internet Explorer): If it starts with https instead of http, your connection is encrypted.

steganography

Steganography, from the Greek for "hidden writing," refers to a variety of methods of sending hidden messages where not only the content of the message is hidden but the very fact that something covert is being sent is also concealed. Usually this is done by concealing something within something else, like a picture or a text about something innocent or completely unrelated. Unlike cryptography, where it is clear that a secret message is being transmitted, steganography does not attract attention to the fact that someone is trying to conceal or encrypt a message.

threat analysis

A security threat analysis is properly a detailed, formal study of all known ways of attacking the security of servers or protocols, or of methods for using them for a particular purpose such as circumvention. Threats can be technical, such as code-breaking or exploiting software bugs, or social, such as stealing passwords or bribing someone who has special knowledge. Few companies or individuals have the knowledge and skill to do a comprehensive threat analysis, but everybody involved in circumvention has to make some estimate of the issues.

Top-Level Domain (TLD)

In Internet names, the TLD is the last component of the domain name. There are several generic TLDs, most notably .com, .org, .edu, .net, .gov, .mil, .int, and one two-letter country code (ccTLD) for each country in the system, such as .ca for Canada. The European Union also has the two-letter code .eu.

TLS (Transport Layer Security)

TLS or Transport Layer Security is a cryptographic standard based on SSL, used to make Internet transactions secure.

TCP/IP (Transmission Control Protocol over Internet Protocol)

TCP and IP are the fundamental protocols of the Internet, handling packet transmission and routing. There are a few alternative protocols that are used at this level of Internet structure, such as UDP.

Tor bridge

A bridge is a middleman Tor node that is not listed in the main public Tor directory, and so is possibly useful in countries where the public relays are blocked. Unlike the case of exit nodes, IP addresses of bridge nodes never appear in server log files and never pass through monitoring nodes in a way that can be connected with circumvention.

traffic analysis

Traffic analysis is statistical analysis of encrypted communications. In some circumstances traffic analysis can reveal information about the people communicating and the information being communicated.

tunnel

A tunnel is an alternate route from one computer to another, usually including a protocol that specifies encryption of messages.

UDP (User Datagram Packet)

UDP is an alternate protocol used with IP. Most Internet services can be accessed using either TCP or UDP, but there are some that are defined to use only one of these alternatives. UDP is especially useful for real-time multimedia applications like Internet phone calls (VoIP).

URL (Uniform Resource Locator)

The URL (Uniform Resource Locator) is the address of a Web site. For example, the URL for the World News section of the NY Times is http://www.nytimes.com/pages/world/index.html. Many censoring systems can block a single URL. Sometimes an easy way to bypass the block is to obscure the URL. It is for example possible to add a dot after the sitename, so the URL http://en.cship.org/wiki/URL becomes http://en.cship.org./wiki/URL. If you are lucky with this little trick you can access blocked Web sites.

Usenet

Usenet is a more than 20-year-old discussion forum system accessed using the NNTP protocol. The messages are not stored on one server but on many servers which distribute their content constantly. Because of that it is impossible to censor Usenet as a whole, however *access* to Usenet can and is often blocked, and any particular server is likely to carry only a subset of locally-acceptable Usenet newsgroups. Google archives the entire available history of Usenet messages for searching.

VoIP (Voice over Internet Protocol)

VoIP refers to any of several protocols for real-time two-way voice communication on the Internet, which is usually much less expensive than calling over telephone company voice networks. It is not subject to the kinds of wiretapping practiced on telephone networks, but can be monitored using digital technology. Many companies produce software and equipment to eavesdrop on VoIP calls; securely encrypted VoIP technologies have only recently begun to emerge.

VPN (virtual private network)

A VPN (virtual private network) is a private communication network used by many companies and organizations to connect securely over a public network. Usually on the Internet it is encrypted and so nobody except the endpoints of the communication can look at the data traffic. There are various standards like IPSec, SSL, TLS or PPTP. The use of a VPN provider is a very fast secure and convenient method to bypass Internet censorship with little risks but it generally costs money every month.

whitelist

A whitelist is a list of sites specifically authorized for a particular form of communication. Filtering traffic can be done either by a whitelist (block everything but the sites on the list), a blacklist (allow everything but the sites on the list), a combination of the two, or by other policies based on specific rules and conditions.

World Wide Web (WWW)

The World Wide Web is the network of hyperlinked domains and content pages accessible using the Hypertext Transfer Protocol and its numerous extensions. The World Wide Web is the most famous part of the Internet.

Webmail

Webmail is e-mail service through a Web site. The service sends and receives mail messages for users in the usual way, but provides a Web interface for reading and managing messages, as an alternative to running a mail client like Outlook Express or Thunderbird on the user's computer. For example a popular and free webmail service is https://mail.google.com/

Web proxy

A Web proxy is a script running on a Web server which acts as a proxy/gateway. Users can access such a Web proxy with their normal Web browser (like Firefox) and enter any URL in the form located on that Web site. Then the Web proxy program on the server receives that Web content and displays it to the user. This way the ISP only sees a connection to the server with the Web proxy since there is no direct connection.

License

All chapters copyright of the authors (see below). Unless otherwise stated all chapters in this manual licensed with **GNU General Public License version 2**.

Authors

ABOUT THIS MANUAL
© adam hyde 2008
Modifications:
Edward Cherlin 2008
Janet Swisher 2008
Tom Boyle 2008
Zorrino Zorrinno 2009

ADVANCED BACKGROUND
© Steven Murdoch And Ross Anderson 2008
Modifications:
adam hyde 2008
Alice Miller 2008
Freerk Ohling 2008
Niels Elgaard Larsen 2009
Sam Tennyson 2008
Seth Schoen 2008
Tom Boyle 2008
Tomas Krag 2008

DETECTION AND ANONYMITY
© Seth Schoen 2008
Modifications:
adam hyde 2008
Alice Miller 2008
Edward Cherlin 2008
Freerk Ohling 2008
Janet Swisher 2008
Sam Tennyson 2008
Tom Boyle 2008
Tomas Krag 2008
Zorrino Zorrinno 2008

RISKS
© Nart Villeneuve 2008
Modifications:
adam hyde 2008
Alice Miller 2008
Freerk Ohling 2008
Janet Swisher 2008
Sam Tennyson 2008
Seth Schoen 2008
Tom Boyle 2008
Tomas Krag 2008

SOCKS PROXIES
© Seth Schoen 2008
Modifications:
adam hyde 2008
Freerk Ohling 2008, 2009
Tom Boyle 2008

USING SWITCH PROXY
© adam hyde 2008, 2009
Modifications:
Alice Miller 2008
Freerk Ohling 2008
Sam Tennyson 2008
Seth Schoen 2008
Tom Boyle 2008

CREDITS
© adam hyde 2006, 2007, 2008
Modifications:
Edward Cherlin 2008

FILTERING TECHNIQUES
© Edward Cherlin 2008
Modifications:
adam hyde 2008
Alice Miller 2008
Janet Swisher 2008
Niels Elgaard Larsen 2009
Sam Tennyson 2008
Seth Schoen 2008
Tom Boyle 2008
Tomas Krag 2008

FURTHER RESOURCES
© adam hyde 2008
Modifications:
Edward Cherlin 2008
Freerk Ohling 2008
Sam Tennyson 2008
Seth Schoen 2008
Tom Boyle 2008
Tomas Krag 2008
Zorrino Zorrinno 2008, 2009

GLOSSARY
© Freerk Ohling 2008
Modifications:
adam hyde 2008
Alice Miller 2008
Edward Cherlin 2008
Janet Swisher 2008
Sam Tennyson 2008
Seth Schoen 2008
Tom Boyle 2008
Tomas Krag 2008

AM I BEING CENSORED?
© adam hyde 2008
Modifications:
Alice Miller 2008

Edward Cherlin 2008
Freerk Ohling 2008
Janet Swisher 2008
Sam Tennyson 2008
Tom Boyle 2008
Zorrino Zorrinno 2008

HOW THE NET WORKS
© Frontline Defenders 2008
Modifications:
adam hyde 2008
Alice Miller 2008
Edward Cherlin 2008
Freerk Ohling 2008
Janet Swisher 2008
Sam Tennyson 2008
Tomas Krag 2008
Zorrino Zorrinno 2008

INSTALLING WEB PROXIES
© Nart Villeneuve 2008
Modifications:
adam hyde 2008
Alice Miller 2008
Edward Cherlin 2008
Freerk Ohling 2008
Sam Tennyson 2008
Seth Schoen 2008
Tom Boyle 2008
Tomas Krag 2008

INSTALLING PHProxy
© Freerk Ohling 2008
Modifications:
adam hyde 2008
Alice Miller 2008
Edward Cherlin 2008
Sam Tennyson 2008
Seth Schoen 2008
Tom Boyle 2008
Tomas Krag 2008

INSTALLING PSIPHON
© Freek Ohling 2008
Modifications:
adam hyde 2008
Alice Miller 2008
Edward Cherlin 2008
Freerk Ohling 2008, 2009
Sam Tennyson 2008
Seth Schoen 2008
Tom Boyle 2008
Tomas Krag 2008
Zorrino Zorrinno 2008

INSTALLING SWITCH PROXY
© adam hyde 2008
Modifications:
Alice Miller 2008
Edward Cherlin 2008
Janet Swisher 2008
Sam Tennyson 2008
Seth Schoen 2008
Tom Boyle 2008

INTRODUCTION
© Alice Miller 2006, 2008
Modifications:
adam hyde 2008
Edward Cherlin 2008
Janet Swisher 2008
Seth Schoen 2008
Tom Boyle 2008

RISKS OF OPERATING A PROXY
© Seth Schoen 2008
Modifications:
adam hyde 2008
Alice Miller 2008
Edward Cherlin 2008
Freerk Ohling 2008
Sam Tennyson 2008
Tom Boyle 2008

SSH TUNNELLING
© Seth Schoen 2008
Modifications:
adam hyde 2008
Alice Miller 2008
Freerk Ohling 2008, 2009
Sam Tennyson 2008
TWikiGuest 2008
Tom Boyle 2008
Tomas Krag 2008
Zorrino Zorrinno 2008

SETTING UP A TOR RELAY
© Zorrino Zorrinno 2008
Modifications:
adam hyde 2008
Alice Miller 2008
Edward Cherlin 2008
Sam Tennyson 2008
Seth Schoen 2008
Tom Boyle 2008
Tomas Krag 2008

SIMPLE TRICKS
© Ronald Deibert 2008
Modifications:
adam hyde 2008
Alice Miller 2008
Edward Cherlin 2008
Freerk Ohling 2008
Janet Swisher 2008
Sam Tennyson 2008
Seth Schoen 2008
Tom Boyle 2008
Tomas Krag 2008
Zorrino Zorrinno 2008

TOR: THE ONION ROUTER
© Zorrino Zorrinno 2008
Modifications:
adam hyde 2008
Alice Miller 2008
Ben Weissmann 2009
Edward Cherlin 2008
Freerk Ohling 2008
Sam Tennyson 2008
Seth Schoen 2008
Tom Boyle 2008
Tomas Krag 2008

USING TOR WITH BRIDGES
© Zorrino Zorrinno 2008
Modifications:
adam hyde 2008
Alice Miller 2008
Edward Cherlin 2008
Freerk Ohling 2008, 2009
Janet Swisher 2008
Sam Tennyson 2008
Seth Schoen 2008
Tom Boyle 2008
Tomas Krag 2008

USING JON DO
© Freerk Ohling 2008
Modifications:
adam hyde 2008
Alice Miller 2008
Sam Tennyson 2008
Tom Boyle 2008
Tomas Krag 2008

OPENVPN
© Tomas Krag 2008
Modifications:
adam hyde 2008
Alice Miller 2008

Freerk Ohling 2008
Sam Tennyson 2008
Seth Schoen 2008

USING PHProxy
© Freerk Ohling 2008
Modifications:
adam hyde 2008
Alice Miller 2008
Janet Swisher 2008
Sam Tennyson 2008
Seth Schoen 2008
Tom Boyle 2008
Zorrino Zorrinno 2008

USING PSIPHON
© Freerk Ohling 2008
Modifications:
adam hyde 2008
Alice Miller 2008
Janet Swisher 2008
Sam Tennyson 2008
Seth Schoen 2008
Tom Boyle 2008
Zorrino Zorrinno 2008

USING PSIPHON2
© Freerk Ohling 2009
Modifications:
Zorrino Zorrinno 2009

USING TOR BROWSER BUNDLE
© Zorrino Zorrinno 2008
Modifications:
adam hyde 2008
Alice Miller 2008
Freerk Ohling 2008
Janet Swisher 2008
Sam Tennyson 2008
Seth Schoen 2008
Tom Boyle 2008
Tomas Krag 2008

USING TOR IM BROWSER BUNDLE
© Zorrino Zorrinno 2008
Modifications:
adam hyde 2008
Alice Miller 2008
Freerk Ohling 2008
Sahal Ansari 2008
Sam Tennyson 2008
Tom Boyle 2008
Tomas Krag 2008

HTTP PROXIES
© adam hyde 2008
Modifications:
Alice Miller 2008
Freerk Ohling 2008
Janet Swisher 2008
Sam Tennyson 2008
Seth Schoen 2008
Tom Boyle 2008
Tomas Krag 2008
Zorrino Zorrinno 2008

USING A WEB PROXY
© Nart Villeneuve 2008
Modifications:
adam hyde 2008
Alice Miller 2008
Freerk Ohling 2008
Janet Swisher 2008
Sam Tennyson 2008
Seth Schoen 2008
Tomas Krag 2008
Zorrino Zorrinno 2008

WHAT IS CIRCUMVENTION
© Ronald Deibert 2008
Modifications:
adam hyde 2008
Alice Miller 2008
Sam Tennyson 2008
Edward Cherlin 2008
Janet Swisher 2008
Sam Tennyson 2008

WHAT IS VPN?
© Nart Villeneuve 2008
Modifications:
adam hyde 2008
Alice Miller 2008
Edward Cherlin 2008
Freerk Ohling 2008
Sam Tennyson 2008
Seth Schoen 2008
Tom Boyle 2008
Tomas Krag 2008

WHO CONTROLS THE NET
© adam hyde 2008
Modifications:
Alice Miller 2008
Edward Cherlin 2008
Freerk Ohling 2008
Janet Swisher 2008
Niels Elgaard Larsen 2009

Sam Tennyson 2008
Seth Schoen 2008
Tomas Krag 2008

Free manuals for free software

General Public License

Version 2, June 1991

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users. This General Public License applies to most of the Free Software Foundation's software and to any other program whose authors commit to using it. (Some other Free Software Foundation software is covered by the GNU Lesser General Public License instead.) You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights. These restrictions translate to certain responsibilities for you if you distribute copies of the software, or if you modify it.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must give the recipients all the rights that you have. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

We protect your rights with two steps: (1) copyright the software, and (2) offer you this license which gives you legal permission to copy, distribute and/or modify the software.

Also, for each author's protection and ours, we want to make certain that everyone understands that there is no warranty for this free software. If the software is modified by someone else and passed on, we want its recipients to know that what they have is not the original, so that any problems introduced by others will not reflect on the original authors' reputations.

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that redistributors of a free program will individually obtain patent licenses, in effect making the program proprietary. To prevent this, we have made it clear that any patent must be licensed for everyone's free use or not licensed at all.

The precise terms and conditions for copying, distribution and modification follow.

TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License. The "Program", below, refers to any such program or work, and a "work based on the Program" means either the Program or any derivative work under copyright law: that is to say, a work containing the Program or a portion of it, either verbatim or with modifications and/or translated into another language. (Hereinafter, translation is included without limitation in the term "modification".) Each licensee is addressed as "you".

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running the Program is not restricted, and the output from the Program is covered only if its contents constitute a work based on the Program (independent of having been made by running the Program). Whether that is true depends on what the Program does.

1. You may copy and distribute verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the Program.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

> **a)** You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.
>
> **b)** You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.
>
> **c)** If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the most ordinary way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this License. (Exception: if the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Program, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Program, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Program.

In addition, mere aggregation of another work not based on the Program with the Program (or with a work based on the Program) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may copy and distribute the Program (or a work based on it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you also do one of the following:

a) Accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

b) Accompany it with a written offer, valid for at least three years, to give any third party, for a charge no more than your cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code, to be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

c) Accompany it with the information you received as to the offer to distribute corresponding source code. (This alternative is allowed only for noncommercial distribution and only if you received the program in object code or executable form with such an offer, in accord with Subsection b above.)

The source code for a work means the preferred form of the work for making modifications to it. For an executable work, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the executable. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as distribution of the source code, even though third parties are not compelled to copy the source along with the object code.

4. You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

5. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Program or works based on it.

6. Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.

7. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent license would not permit royalty-free redistribution of the Program by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

8. If the distribution and/or use of the Program is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Program under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

9. The Free Software Foundation may publish revised and/or new versions of the General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Program specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of this License, you may choose any version ever published by the Free Software Foundation.

10. If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

11. BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

12. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS